How to Be a Better Consumer of Security Maturity Models

October 21, 2014

Julia Allen & Dr. Nader Mehravari
Cyber Risk Management Group
Software Engineering Institute
Carnegie Mellon University
http://www.cert.org/resilience/

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **21 OCT 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE
How to Be a Better Consumer of Security Maturity Models

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Allen /Nader Mehravari Julia

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

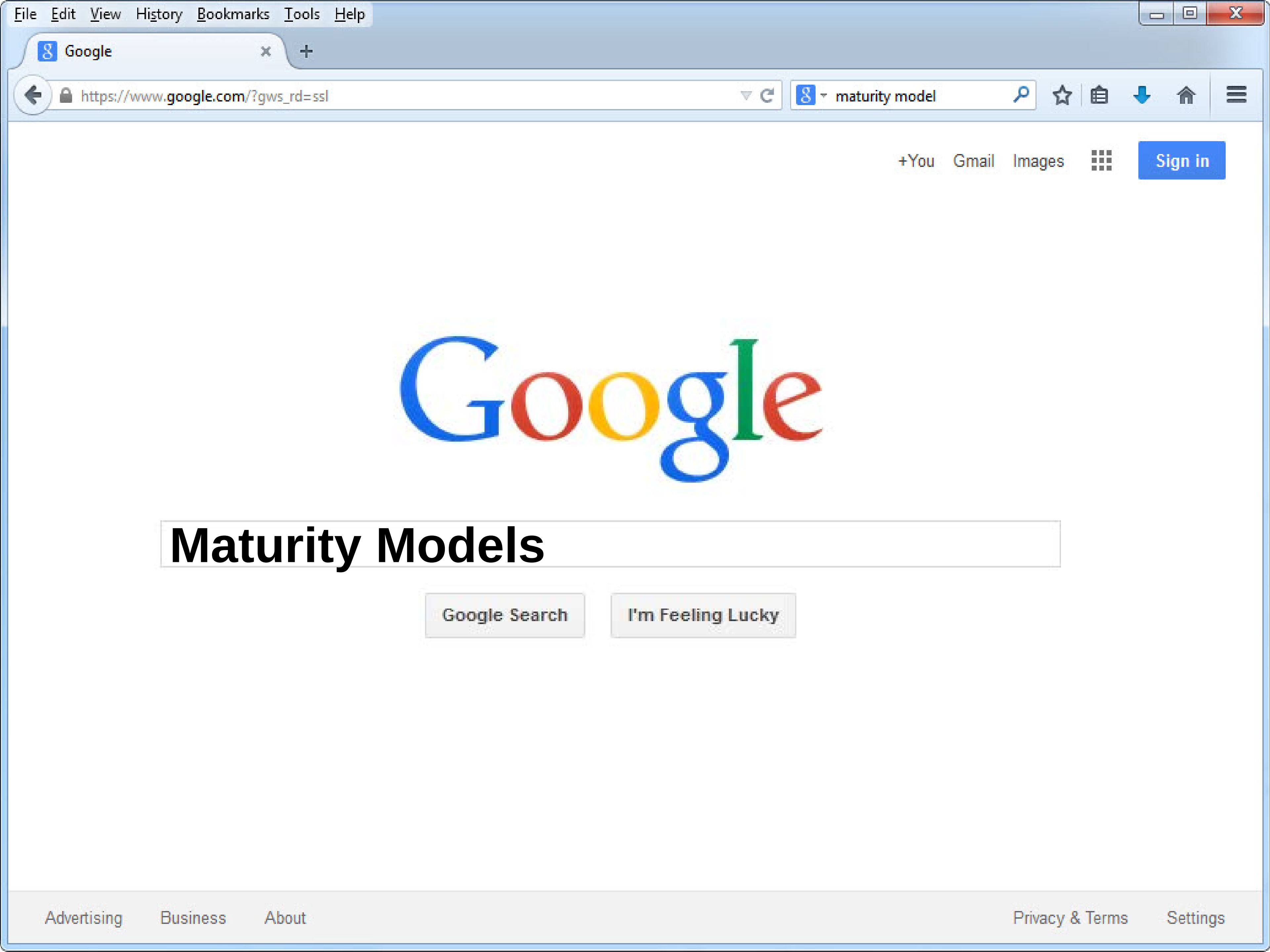
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

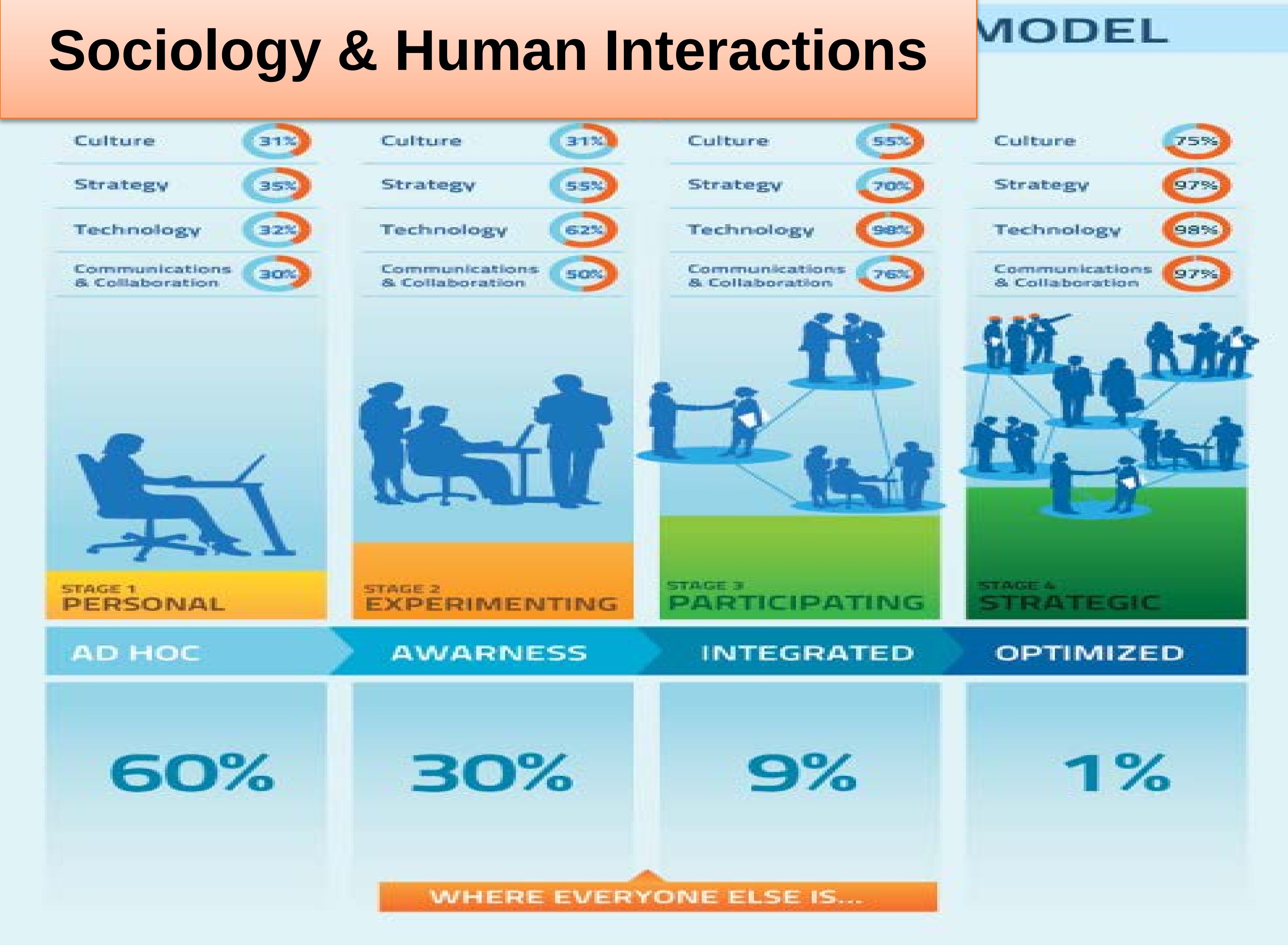
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**82**	



Maturity Models

Sociology & Human Interactions



Culture	31%	31%	55%	75%
Strategy	35%	55%	70%	97%
Technology	32%	62%	98%	98%
Communications & Collaboration	30%	50%	76%	97%
	STAGE 1 PERSONAL	STAGE 2 EXPERIMENTING	STAGE 3 PARTICIPATING	STAGE 4 STRATEGIC
	AD HOC	AWARNESS	INTEGRATED	OPTIMIZED
	60%	30%	9%	1%

WHERE EVERYONE ELSE IS...

Australian Government
Comcover

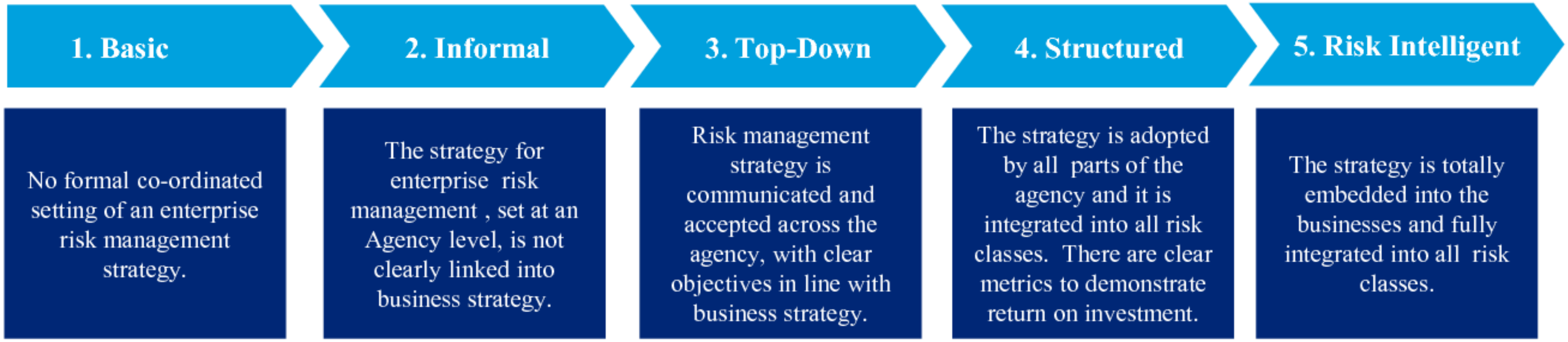
Risk

Risk maturity model

1

The new approach is based on the concept of five levels of Risk Management maturity. These depict the evolution of risk management capability resulting from the actions of management and the investment in enterprise risk management frameworks, systems, people and processes

Example – high level characteristics for each maturity level for ‘Policy and Objectives’ element

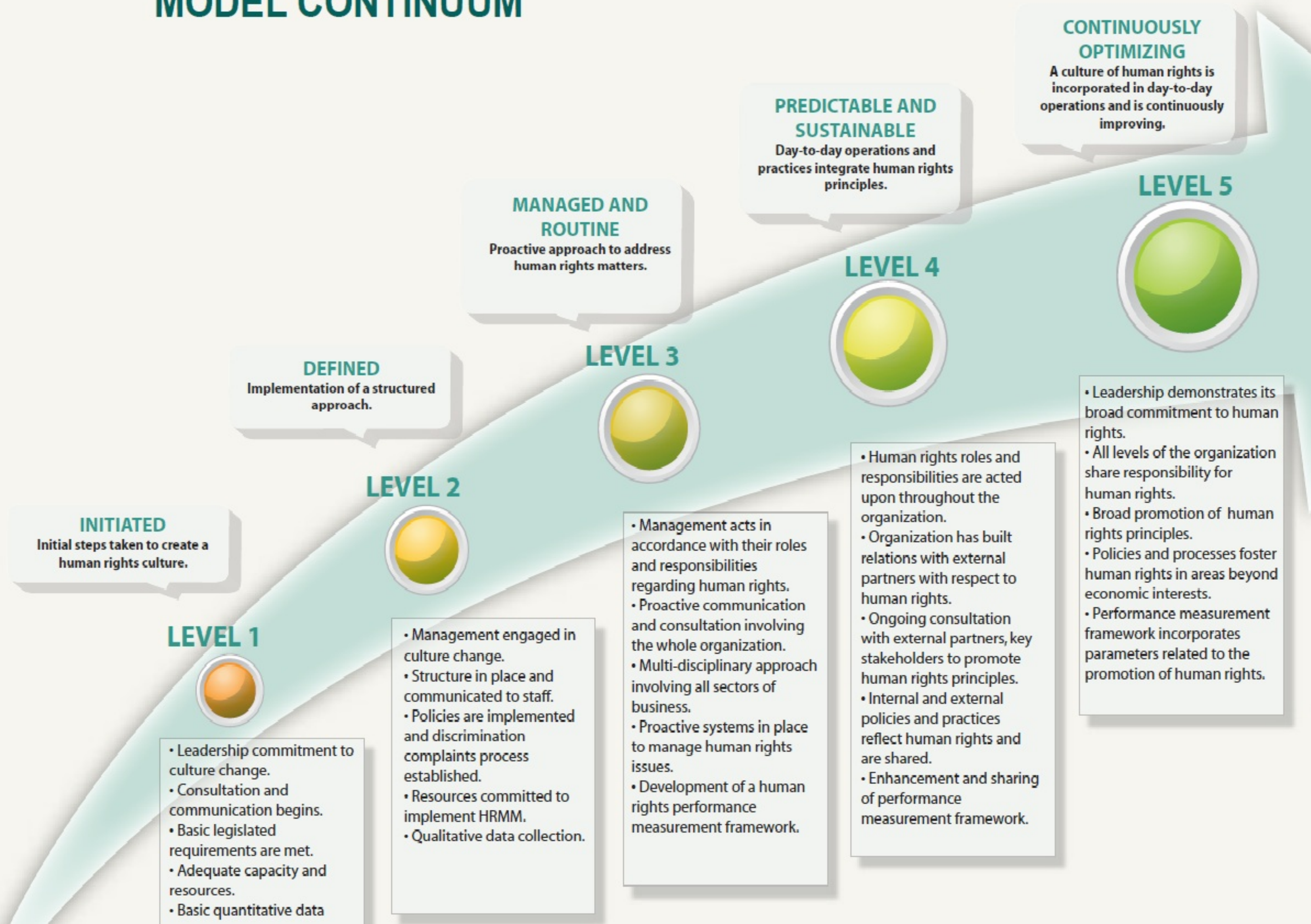


1. Basic	2. Informal	3. Top-Down	4. Structured	5. Risk Intelligent
No formal co-ordinated setting of an enterprise risk management strategy.	The strategy for enterprise risk management , set at an Agency level, is not clearly linked into business strategy.	Risk management strategy is communicated and accepted across the agency, with clear objectives in line with business strategy.	The strategy is adopted by all parts of the agency and it is integrated into all risk classes. There are clear metrics to demonstrate return on investment.	The strategy is totally embedded into the businesses and fully integrated into all risk classes.

CANADIAN HUMAN RIGHTS COMMISSION

Human Rights

HUMAN RIGHTS MATURITY MODEL CONTINUUM



LEVEL 1

INITIATED
Initial steps taken to create a human rights culture.

- Leadership commitment to culture change.
- Consultation and communication begins.
- Basic legislated requirements are met.
- Adequate capacity and resources.
- Basic quantitative data

LEVEL 2

DEFINED
Implementation of a structured approach.

- Management engaged in culture change.
- Structure in place and communicated to staff.
- Policies are implemented and discrimination complaints process established.
- Resources committed to implement HRMM.
- Qualitative data collection.

LEVEL 3

MANAGED AND ROUTINE
Proactive approach to address human rights matters.

- Management acts in accordance with their roles and responsibilities regarding human rights.
- Proactive communication and consultation involving the whole organization.
- Multi-disciplinary approach involving all sectors of business.
- Proactive systems in place to manage human rights issues.
- Development of a human rights performance measurement framework.

LEVEL 4

PREDICTABLE AND SUSTAINABLE
Day-to-day operations and practices integrate human rights principles.

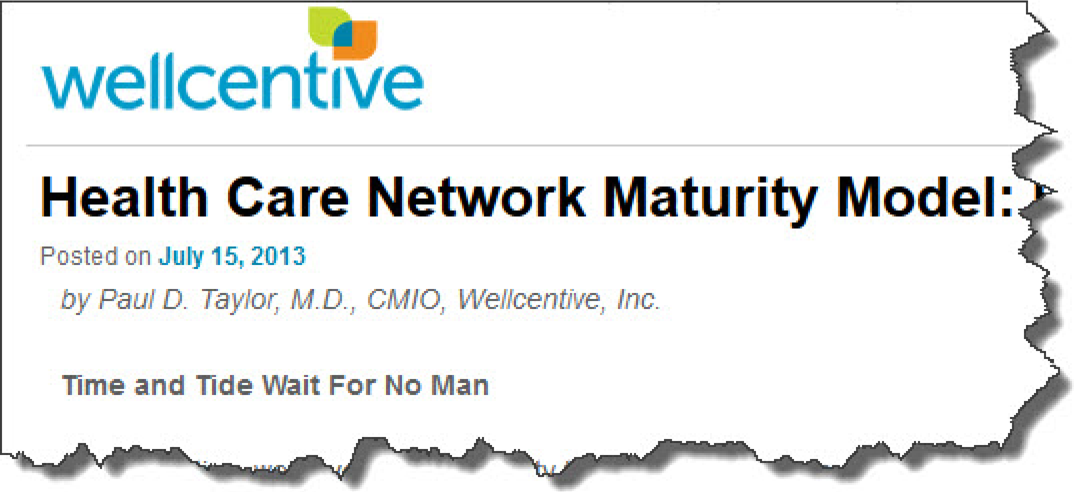
- Human rights roles and responsibilities are acted upon throughout the organization.
- Organization has built relations with external partners with respect to human rights.
- Ongoing consultation with external partners, key stakeholders to promote human rights principles.
- Internal and external policies and practices reflect human rights and are shared.
- Enhancement and sharing of performance measurement framework.

LEVEL 5

CONTINUOUSLY OPTIMIZING
A culture of human rights is incorporated in day-to-day operations and is continuously improving.

- Leadership demonstrates its broad commitment to human rights.
- All levels of the organization share responsibility for human rights.
- Broad promotion of human rights principles.
- Policies and processes foster human rights in areas beyond economic interests.
- Performance measurement framework incorporates parameters related to the promotion of human rights.

Health Care



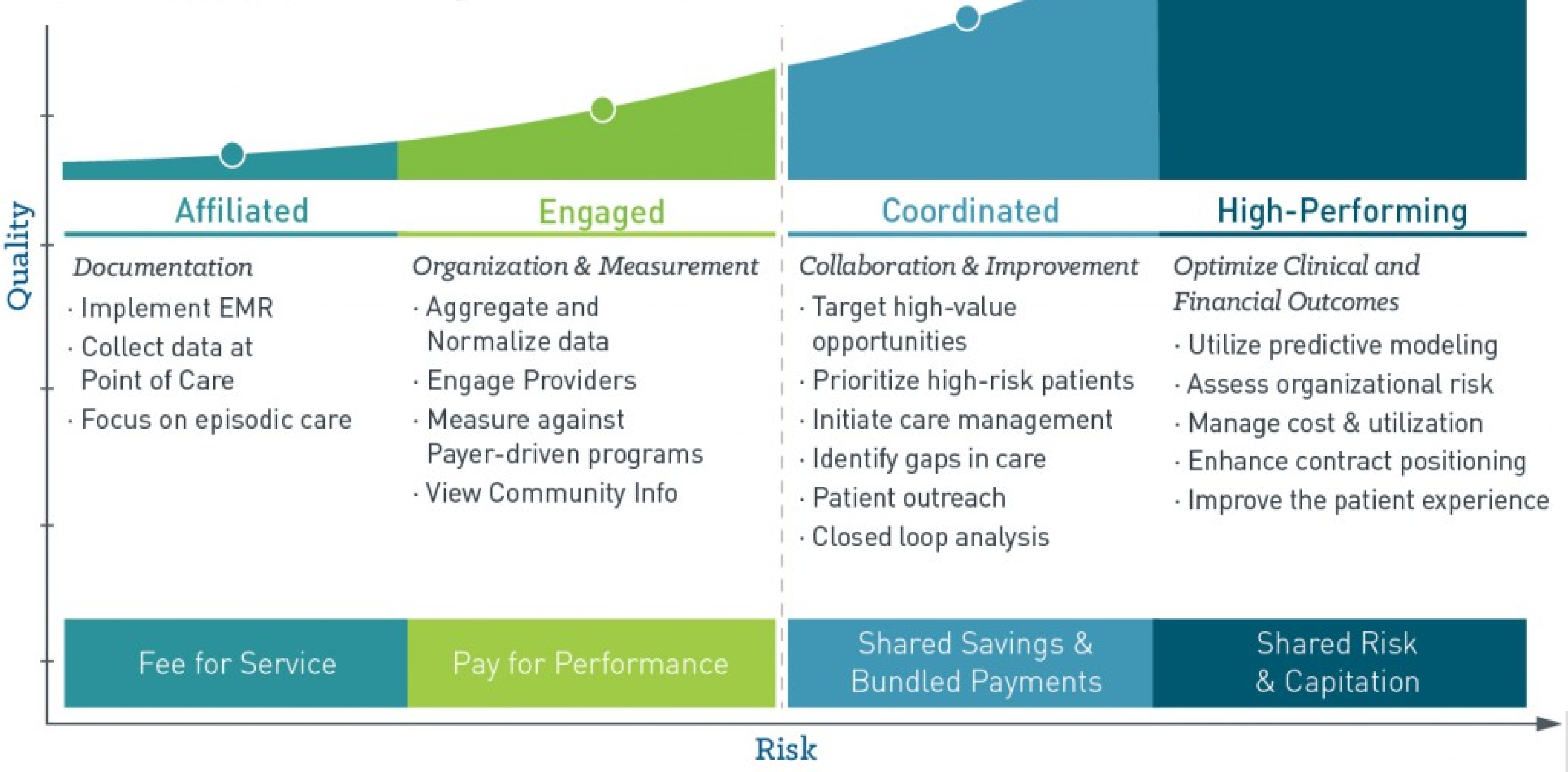
wellcentive

Health Care Network Maturity Model:

Posted on July 15, 2013

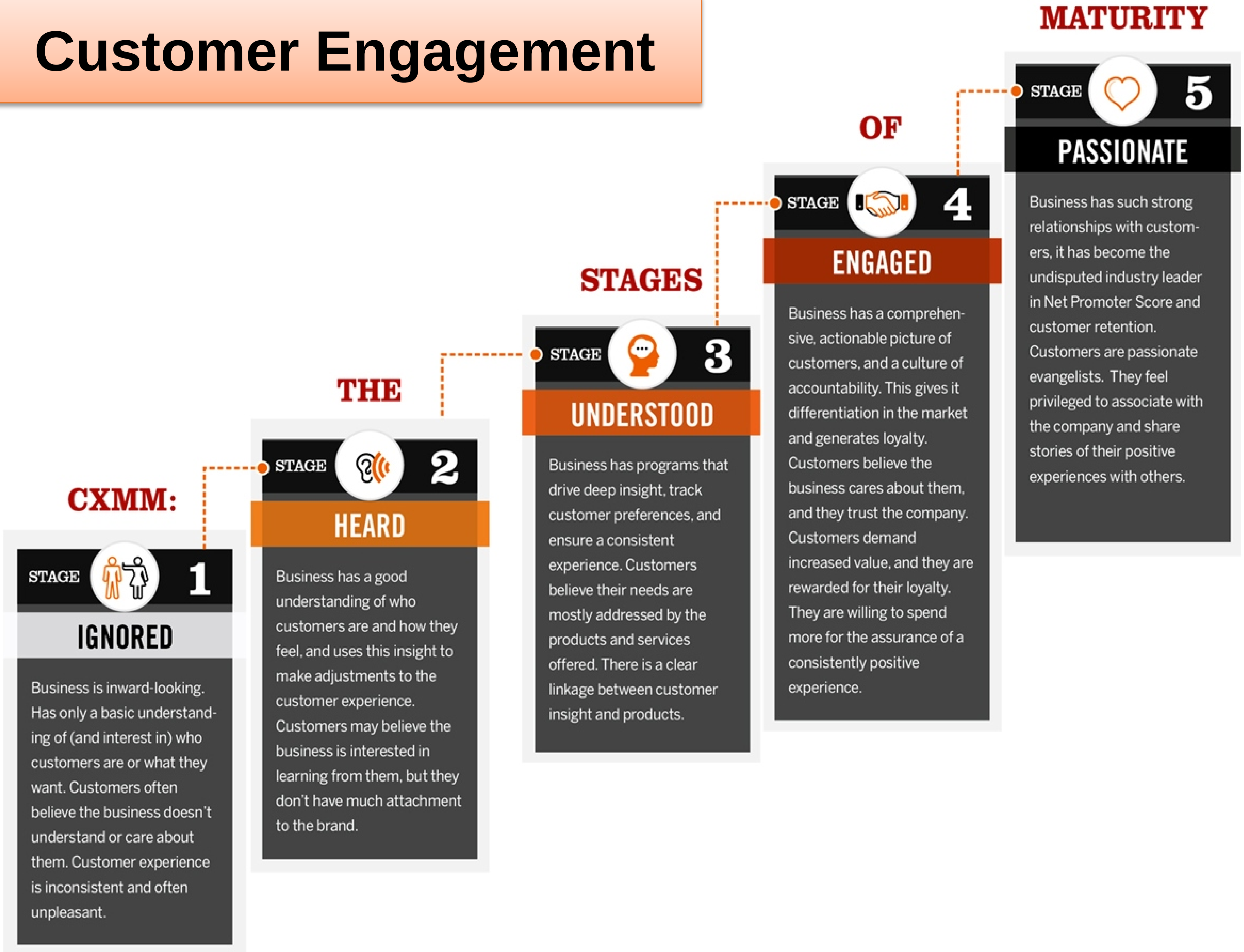
by Paul D. Taylor, M.D., CMIO, Wellcentive, Inc.

Time and Tide Wait For No Man



Affiliated	Engaged	Coordinated	High-Performing
Documentation	*Organization & Measurement*	*Collaboration & Improvement*	*Optimize Clinical and Financial Outcomes*
· Implement EMR · Collect data at Point of Care · Focus on episodic care	· Aggregate and Normalize data · Engage Providers · Measure against Payer-driven programs · View Community Info	· Target high-value opportunities · Prioritize high-risk patients · Initiate care management · Identify gaps in care · Patient outreach · Closed loop analysis	· Utilize predictive modeling · Assess organizational risk · Manage cost & utilization · Enhance contract positioning · Improve the patient experience
Fee for Service	Pay for Performance	Shared Savings & Bundled Payments	Shared Risk & Capitation

Customer Engagement



CXMM: THE STAGES OF MATURITY

STAGE 1

IGNORED

Business is inward-looking. Has only a basic understanding of (and interest in) who customers are or what they want. Customers often believe the business doesn't understand or care about them. Customer experience is inconsistent and often unpleasant.

STAGE 2

HEARD

Business has a good understanding of who customers are and how they feel, and uses this insight to make adjustments to the customer experience. Customers may believe the business is interested in learning from them, but they don't have much attachment to the brand.

STAGE 3

UNDERSTOOD

Business has programs that drive deep insight, track customer preferences, and ensure a consistent experience. Customers believe their needs are mostly addressed by the products and services offered. There is a clear linkage between customer insight and products.

STAGE 4

ENGAGED

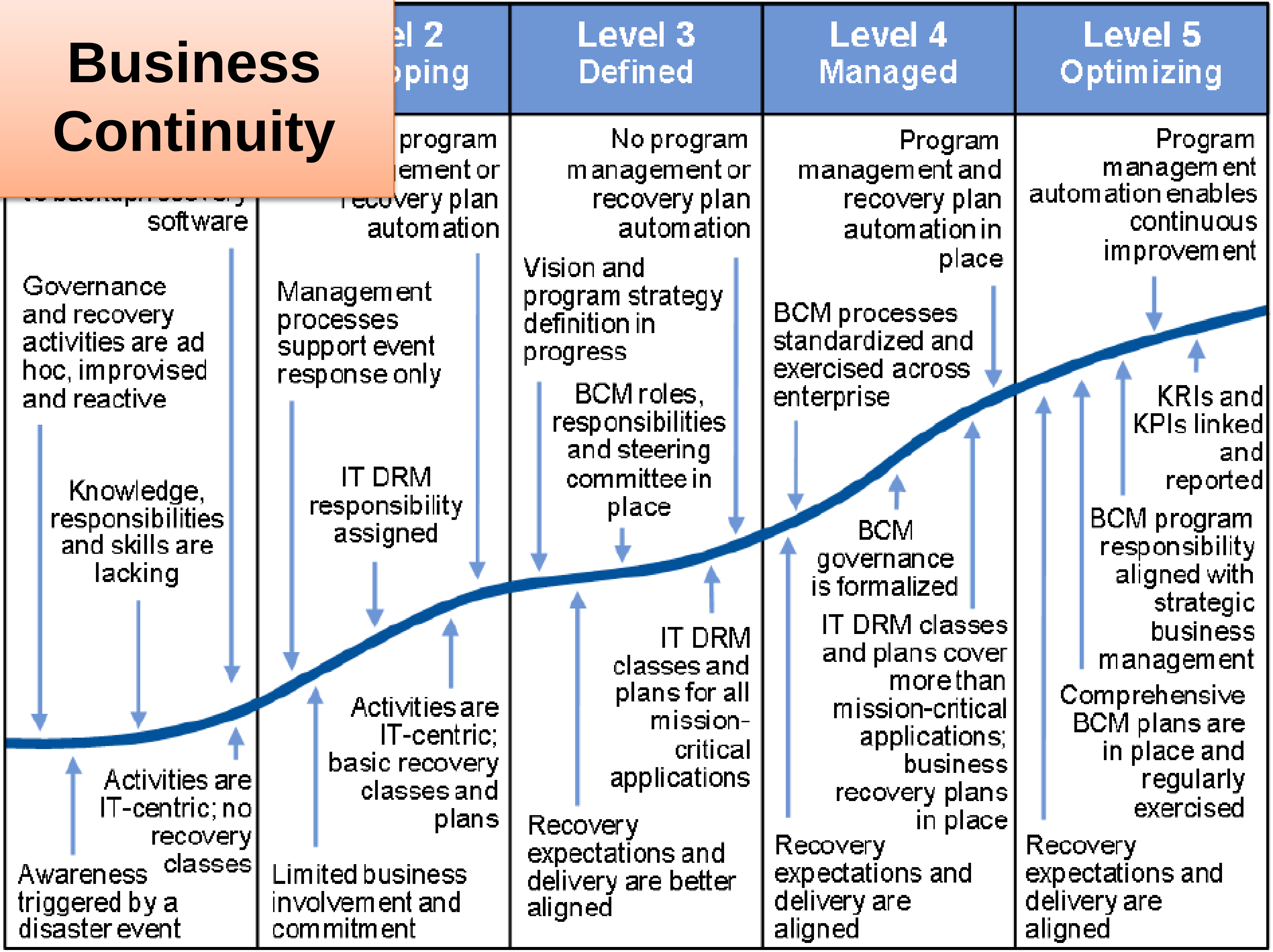
Business has a comprehensive, actionable picture of customers, and a culture of accountability. This gives it differentiation in the market and generates loyalty. Customers believe the business cares about them, and they trust the company. Customers demand increased value, and they are rewarded for their loyalty. They are willing to spend more for the assurance of a consistently positive experience.

STAGE 5

PASSIONATE

Business has such strong relationships with customers, it has become the undisputed industry leader in Net Promoter Score and customer retention. Customers are passionate evangelists. They feel privileged to associate with the company and share stories of their positive experiences with others.

Business Continuity



el 2
ping

Level 3
Defined

Level 4
Managed

Level 5
Optimizing

to backup/recovery software

Governance and recovery activities are ad hoc, improvised and reactive

Knowledge, responsibilities and skills are lacking

Activities are IT-centric; no recovery classes

Awareness triggered by a disaster event

program
gement or
recovery plan
automation

Management processes support event response only

IT DRM responsibility assigned

Activities are IT-centric; basic recovery classes and plans

Limited business involvement and commitment

No program management or recovery plan automation

Vision and program strategy definition in progress

BCM roles, responsibilities and steering committee in place

IT DRM classes and plans for all mission-critical applications

Recovery expectations and delivery are better aligned

Program management and recovery plan automation in place

BCM processes standardized and exercised across enterprise

BCM governance is formalized

IT DRM classes and plans cover more than mission-critical applications; business recovery plans in place

Recovery expectations and delivery are aligned

Program management automation enables continuous improvement

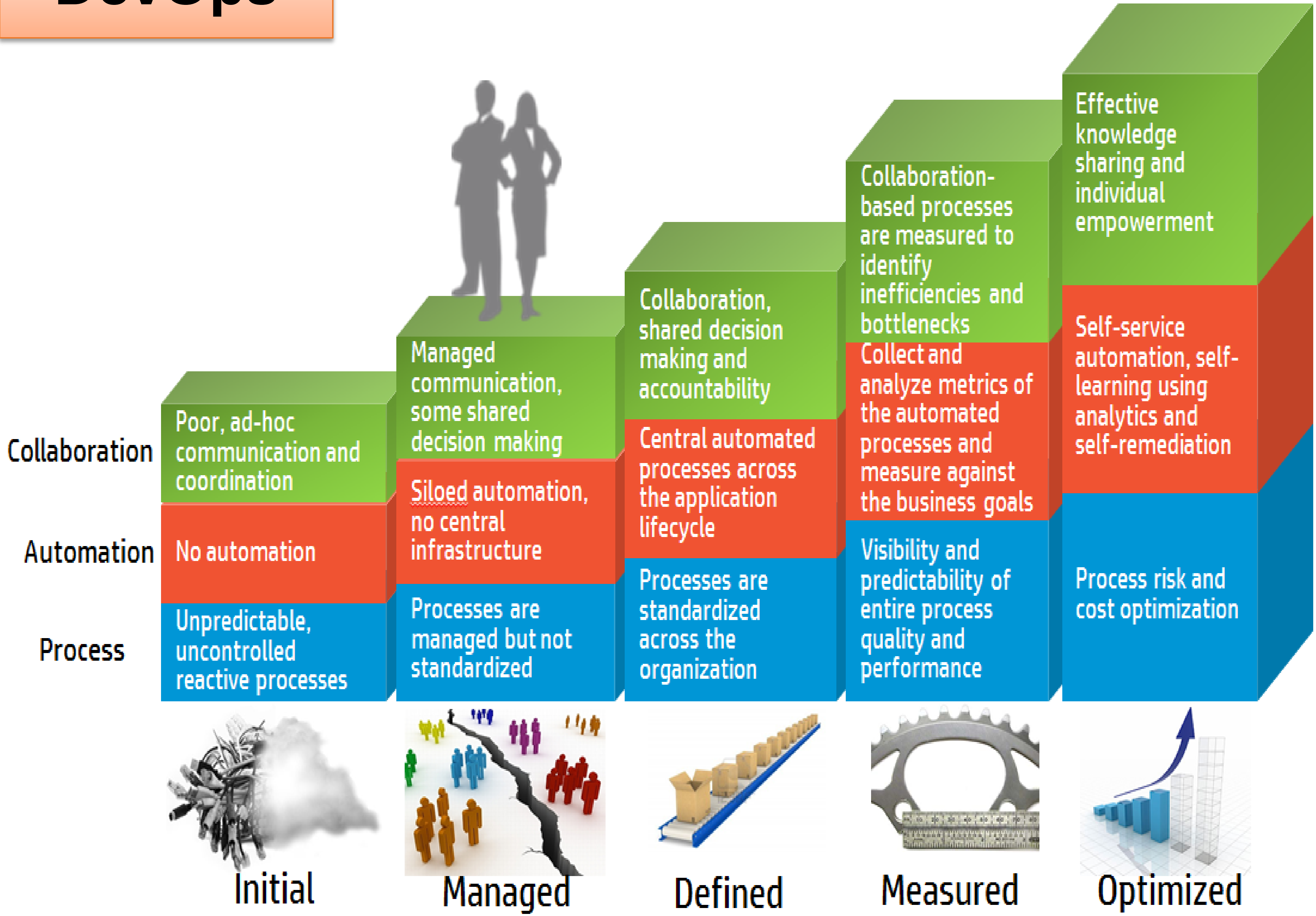
KRIs and KPIs linked and reported

BCM program responsibility aligned with strategic business management

Comprehensive BCM plans are in place and regularly exercised

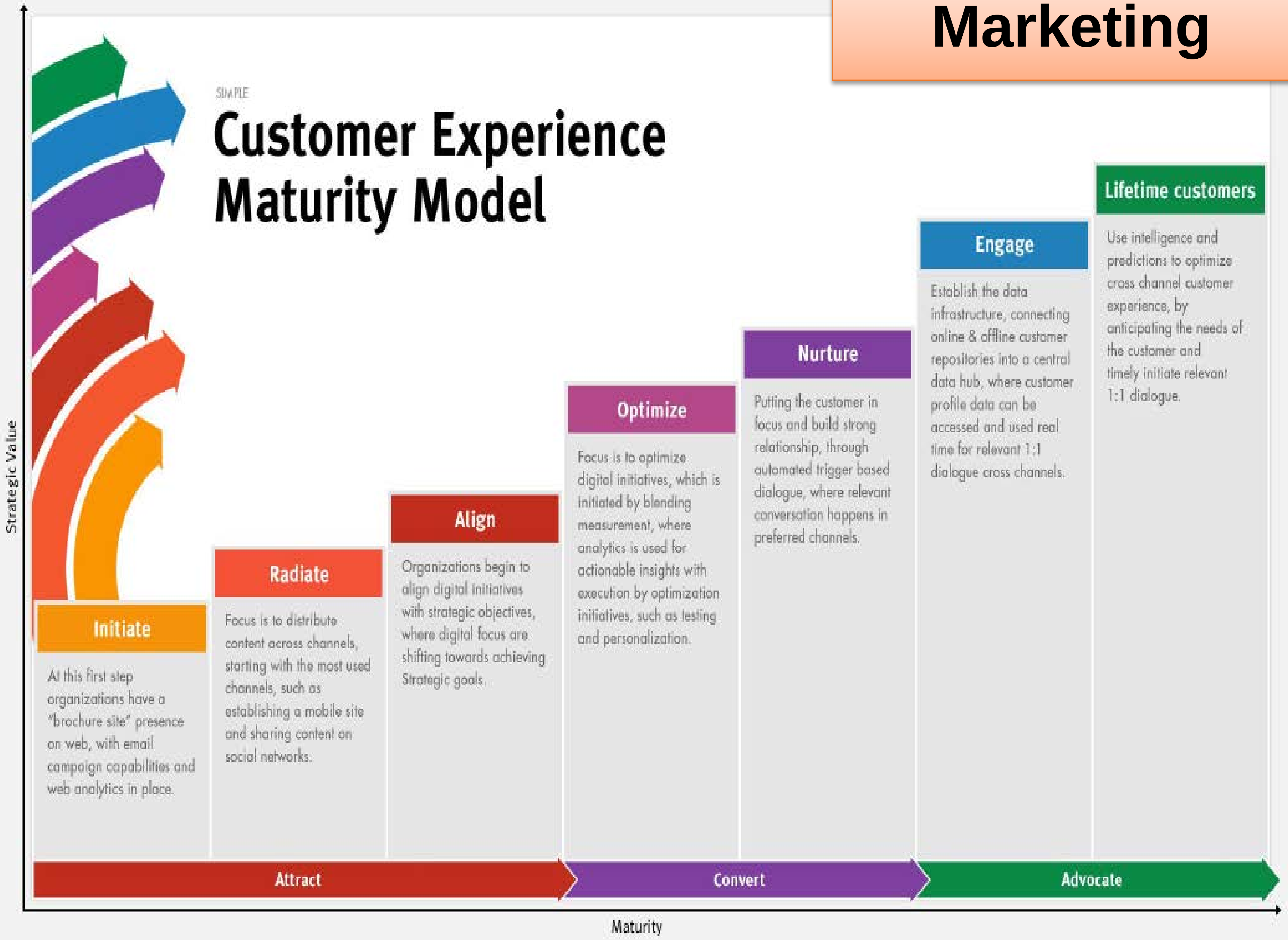
Recovery expectations and delivery are aligned

DevOps



	Initial	Managed	Defined	Measured	Optimized
Collaboration	Poor, ad-hoc communication and coordination	Managed communication, some shared decision making	Collaboration, shared decision making and accountability	Collaboration-based processes are measured to identify inefficiencies and bottlenecks	Effective knowledge sharing and individual empowerment
Automation	No automation	Siloed automation, no central infrastructure	Central automated processes across the application lifecycle	Collect and analyze metrics of the automated processes and measure against the business goals	Self-service automation, self-learning using analytics and self-remediation
Process	Unpredictable, uncontrolled reactive processes	Processes are managed but not standardized	Processes are standardized across the organization	Visibility and predictability of entire process quality and performance	Process risk and cost optimization

Marketing



SIMPLE

Customer Experience Maturity Model

Initiate

At this first step organizations have a "brochure site" presence on web, with email campaign capabilities and web analytics in place.

Radiate

Focus is to distribute content across channels, starting with the most used channels, such as establishing a mobile site and sharing content on social networks.

Align

Organizations begin to align digital initiatives with strategic objectives, where digital focus are shifting towards achieving Strategic goals.

Optimize

Focus is to optimize digital initiatives, which is initiated by blending measurement, where analytics is used for actionable insights with execution by optimization initiatives, such as testing and personalization.

Nurture

Putting the customer in focus and build strong relationship, through automated trigger based dialogue, where relevant conversation happens in preferred channels.

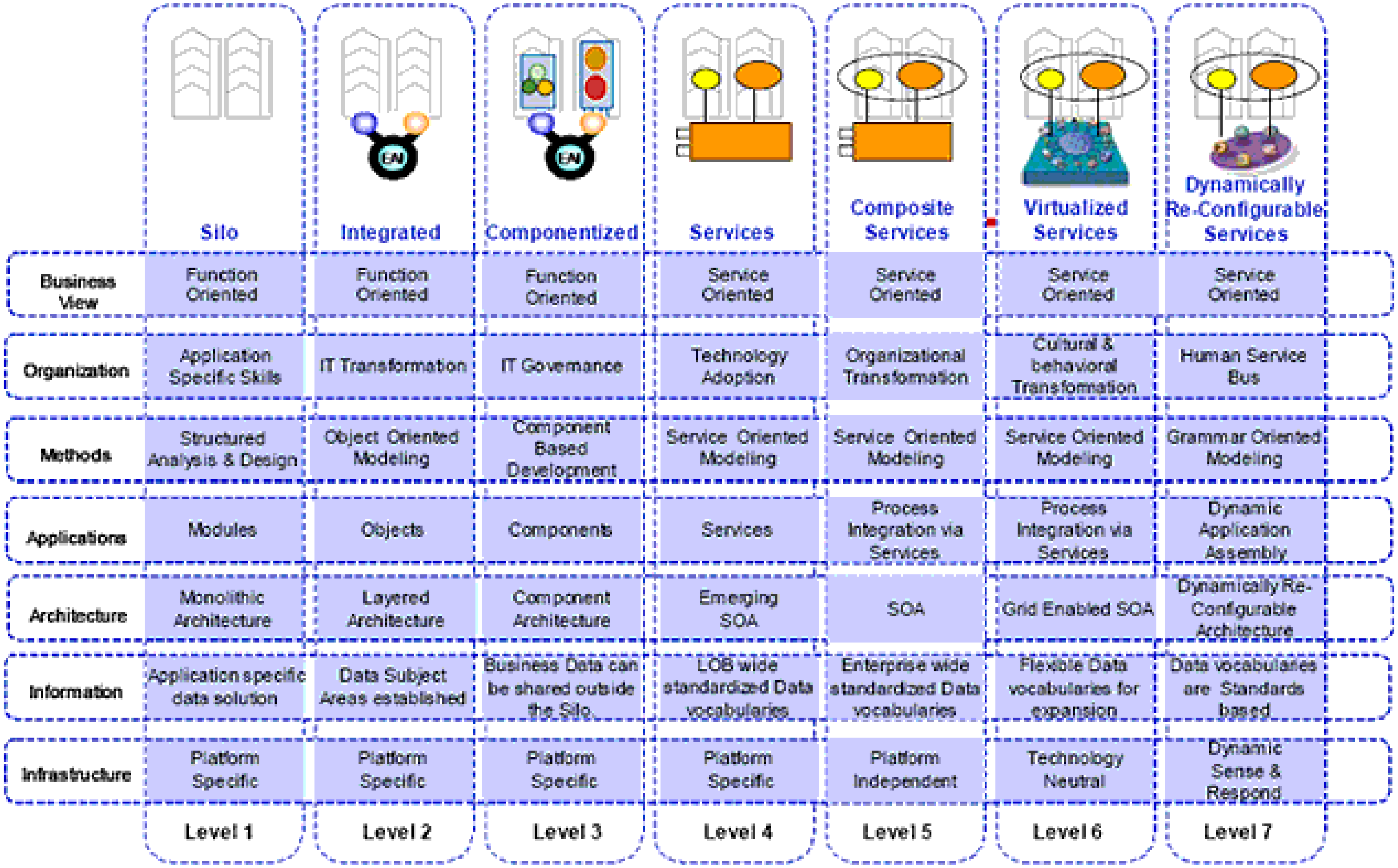
Engage

Establish the data infrastructure, connecting online & offline customer repositories into a central data hub, where customer profile data can be accessed and used real time for relevant 1:1 dialogue cross channels.

Lifetime customers

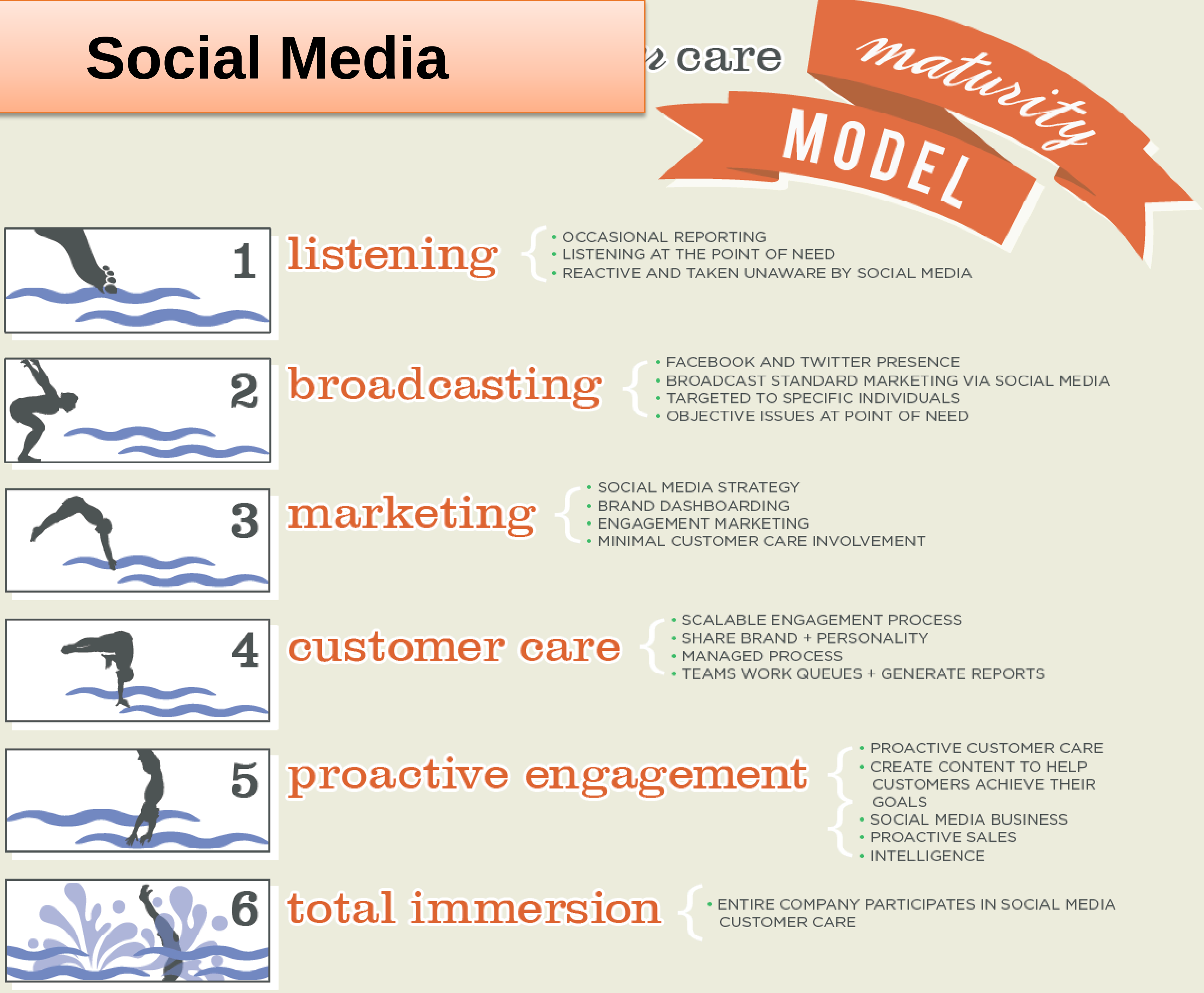
Use intelligence and predictions to optimize cross channel customer experience, by anticipating the needs of the customer and timely initiate relevant 1:1 dialogue.

Service Integration



	Silo	Integrated	Componentized	Services	Composite Services	Virtualized Services	Dynamically Re-Configurable Services
Business View	Function Oriented	Function Oriented	Function Oriented	Service Oriented	Service Oriented	Service Oriented	Service Oriented
Organization	Application Specific Skills	IT Transformation	IT Governance	Technology Adoption	Organizational Transformation	Cultural & behavioral Transformation	Human Service Bus
Methods	Structured Analysis & Design	Object Oriented Modeling	Component Based Development	Service Oriented Modeling	Service Oriented Modeling	Service Oriented Modeling	Grammar Oriented Modeling
Applications	Modules	Objects	Components	Services	Process Integration via Services	Process Integration via Services	Dynamic Application Assembly
Architecture	Monolithic Architecture	Layered Architecture	Component Architecture	Emerging SOA	SOA	Grid Enabled SOA	Dynamically Re-Configurable Architecture
Information	Application specific data solution	Data Subject Areas established	Business Data can be shared outside the Silo	LOB wide standardized Data vocabularies	Enterprise wide standardized Data vocabularies	Flexible Data vocabularies for expansion	Data vocabularies are Standards based
Infrastructure	Platform Specific	Platform Specific	Platform Specific	Platform Specific	Platform Independent	Technology Neutral	Dynamic Sense & Respond
	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7

Social Media



n care maturity MODEL

1 listening
- OCCASIONAL REPORTING
- LISTENING AT THE POINT OF NEED
- REACTIVE AND TAKEN UNAWARE BY SOCIAL MEDIA

2 broadcasting
- FACEBOOK AND TWITTER PRESENCE
- BROADCAST STANDARD MARKETING VIA SOCIAL MEDIA
- TARGETED TO SPECIFIC INDIVIDUALS
- OBJECTIVE ISSUES AT POINT OF NEED

3 marketing
- SOCIAL MEDIA STRATEGY
- BRAND DASHBOARDING
- ENGAGEMENT MARKETING
- MINIMAL CUSTOMER CARE INVOLVEMENT

4 customer care
- SCALABLE ENGAGEMENT PROCESS
- SHARE BRAND + PERSONALITY
- MANAGED PROCESS
- TEAMS WORK QUEUES + GENERATE REPORTS

5 proactive engagement
- PROACTIVE CUSTOMER CARE
- CREATE CONTENT TO HELP CUSTOMERS ACHIEVE THEIR GOALS
- SOCIAL MEDIA BUSINESS
- PROACTIVE SALES
- INTELLIGENCE

6 total immersion
- ENTIRE COMPANY PARTICIPATES IN SOCIAL MEDIA CUSTOMER CARE

Objectives of This Session

Maturity models are effective **tools for improving an organization's security capabilities and outcomes**. But knowing which model to use and how to use it is paramount to success.

- Improve your understanding of **maturity model concepts**
- Learn about the use of maturity models by examining recent **examples** in the cybersecurity and resilience domains
- Be aware of **caution flags** when dealing with maturity models
- Determine **how to choose** the right model for your specific needs (improvement vs. assessment, etc.)

Overall Outline of This Session

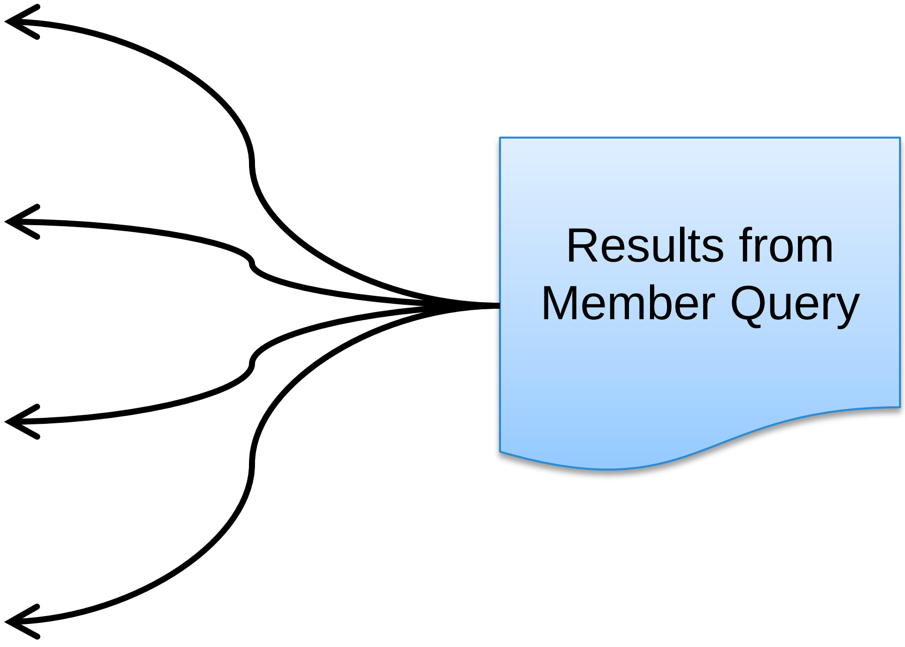
Setting the Stage

Background and History

ABCs of Maturity Models

Panel Discussion

Closing Thoughts



Results from Member Query

Maturity Models Member Query

1	Have you or your organization ever used any type of maturity model?

If yes:

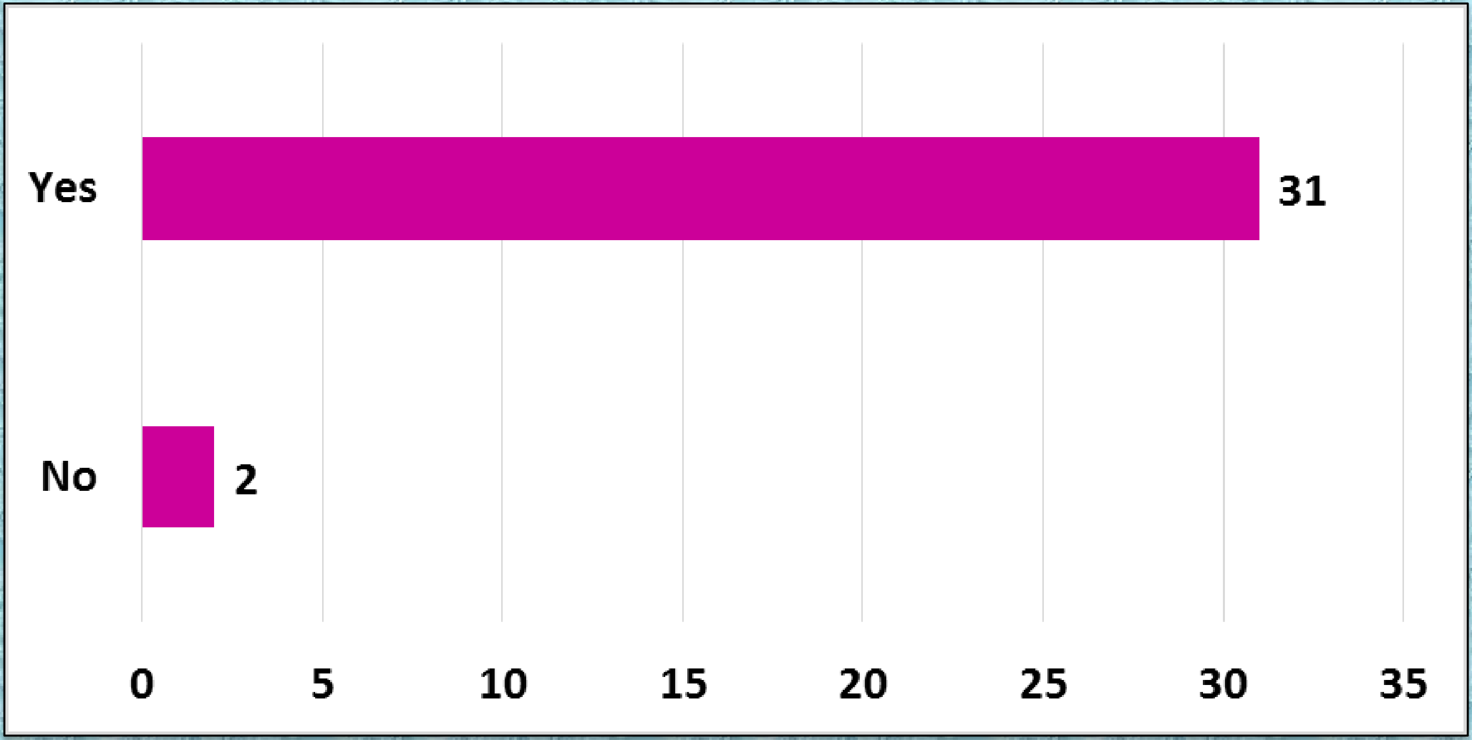
2	In what areas?
3	For what purposes?
4	What were the reasons?
5	Which maturity models?

If no:

6	How do you assess the maturity of your cybersecurity program?

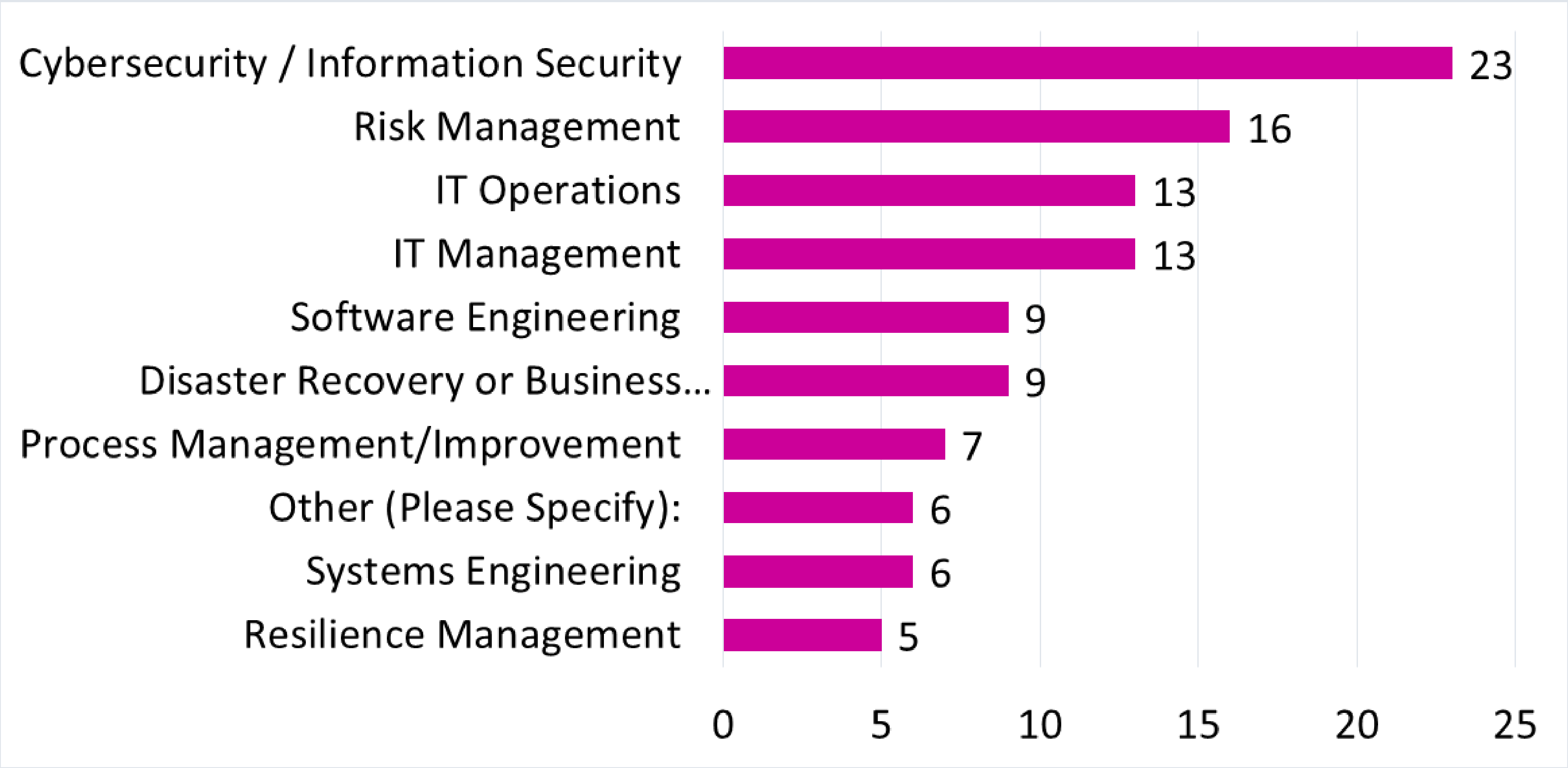
Maturity Models Member Query – Q1

Have you or your organization ever used any type of maturity model?



Maturity Models Member Query – Q2

In what areas?



Maturity Models Member Query – Q2

In what areas?

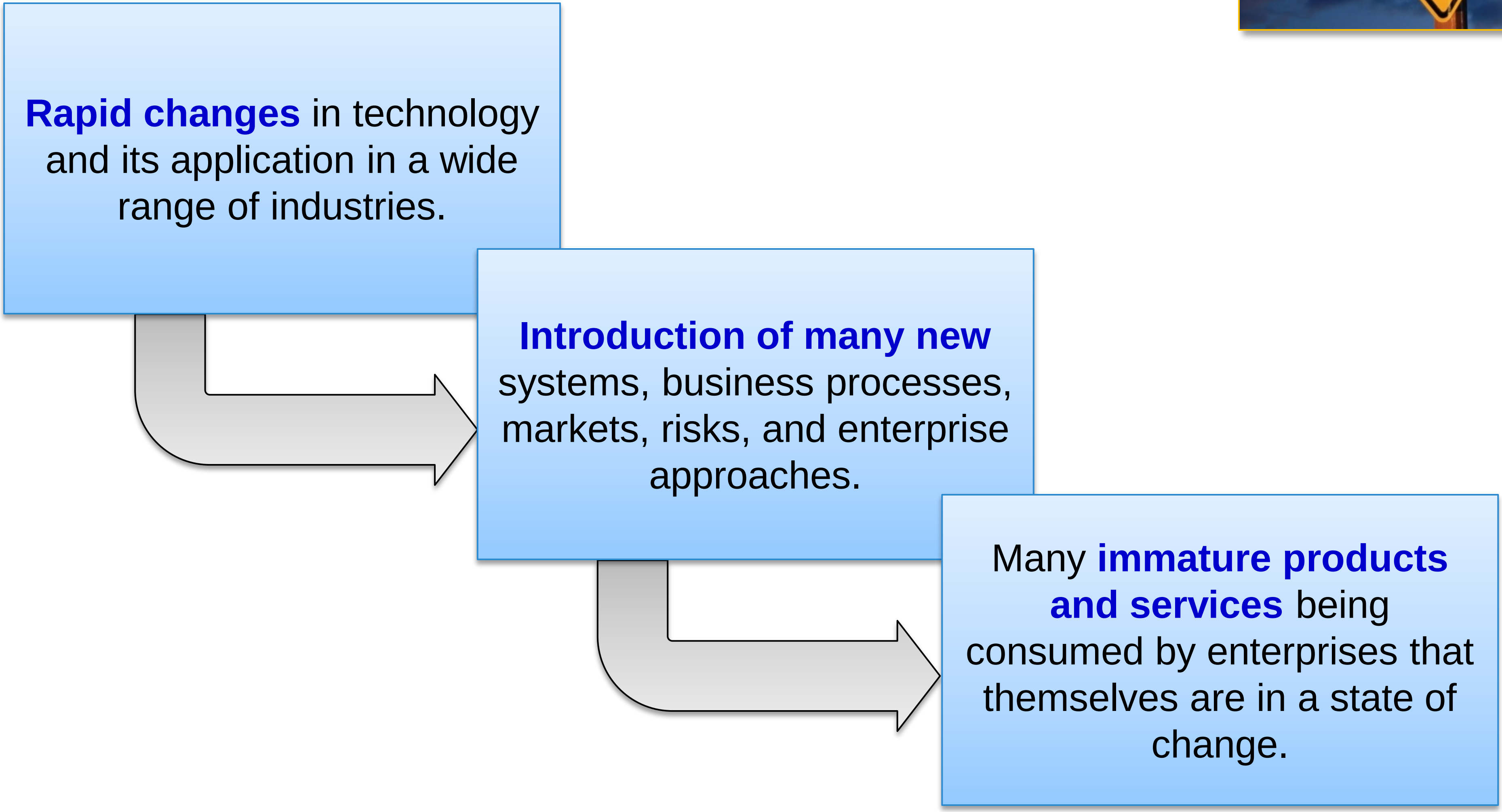
OTHER:

- Client specific projects
- IT architecture
- Incidence response
- Identify and access management
- Product development
- Roadmap activities
- Access one's ability to deal with risk
- Build best practices
- As a very large company, the use of maturity models varies greatly not only from area to area but also from group to group even within the same area.

Setting the Stage

- The need for “measuring” operational activities & their effectiveness
- Are we doing the right things?
- Are we using the right tools to measure?
- Are we measuring the right things?

Today’s Operating Environment



Rapid changes in technology and its application in a wide range of industries.

Introduction of many new systems, business processes, markets, risks, and enterprise approaches.

Many **immature products and services** being consumed by enterprises that themselves are in a state of change.

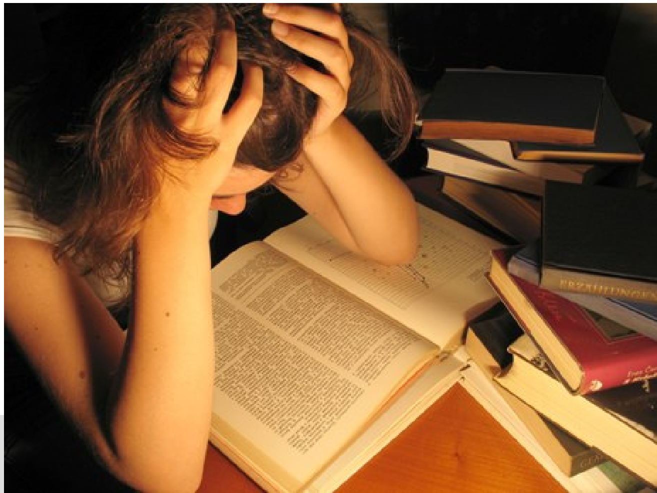
Challenges at Hand

How can you tell if you are doing a good job of managing these changes?

What are effective ways to monitor your progress?

How do you manage the interactions of systems and processes that are continually changing?

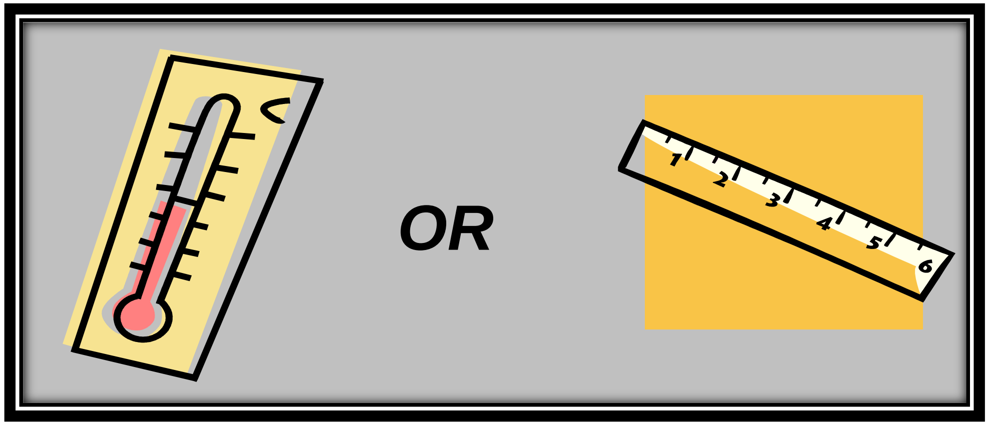
How do poor processes impact interoperability, safety, reliability, efficiency, and effectiveness?



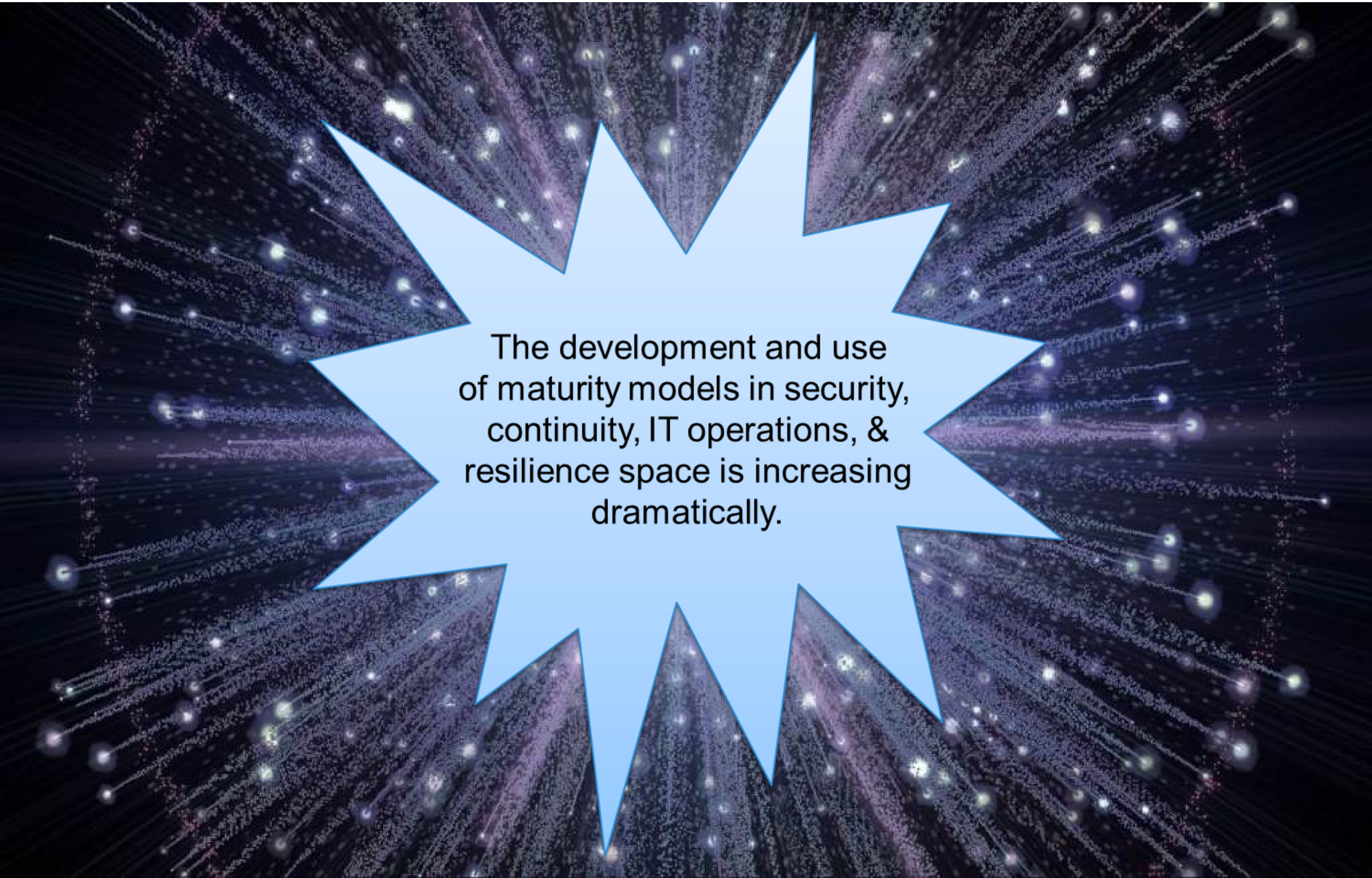
Which Tool Should I Use?

Your organization wants to know **SOMETHING** about your mission operation:

- How **EFFECTIVE** are we?
- Do we have the right **SKILLS** and **CAPABILITIES**?
- Do we have the right **TECHNOLOGIES**?



Observation

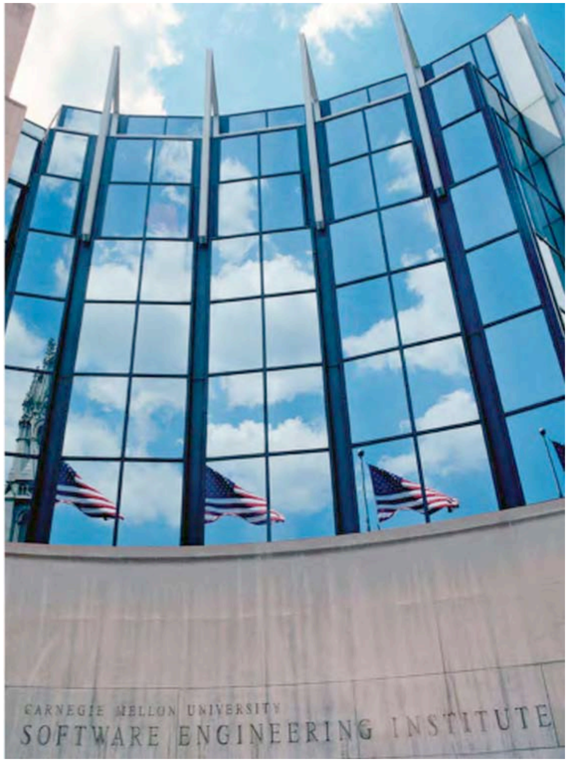


The development and use of maturity models in security, continuity, IT operations, & resilience space is increasing dramatically.

Do Maturity Models Measure the Right Thing?

- **May not measure what you think it measures**
  - Practice maturity vs. organizational maturity?
- **May give you inaccurate data on which to base decisions**
  - Process performance vs. product performance?
- **Can increase cost without increasing benefit**
  - An improved process may not result in compliance
- **May provide a false sense of confidence**
  - A robust process may not improve malware management

CMU – SEI – CERT®



Carnegie
Mellon
University

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT® – *Anticipating and solving our nation’s cybersecurity challenges*

- Largest technical program at SEI
- Focused on internet security, digital investigation, secure systems, insider threat, operational resilience, vulnerability analysis, network situational awareness, and coordinated response

Cyber Risk and Resilience Management Team

Engaged in

- Applied research
- Education & training
- Putting into practice
- Enabling our federal, state, and commercial partners

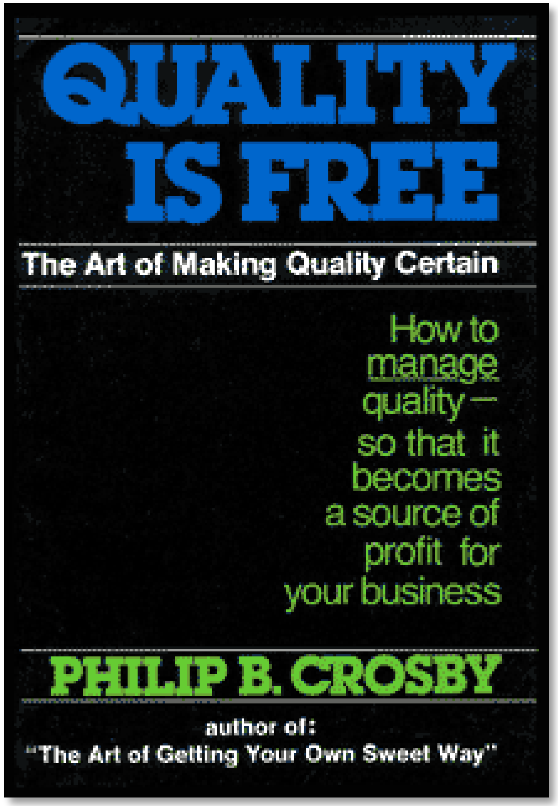
In areas dealing with

- Maturity models
- Operational resilience
- Resilience management
- Operation risk management
- Cybersecurity maturity models
- Integration of cybersecurity, business continuity, & disaster recovery

Background and History

- Where do maturity models come from?
- Early development and instantiation

In the Beginning There Was “Quality is Free”



QUALITY IS FREE

The Art of Making Quality Certain

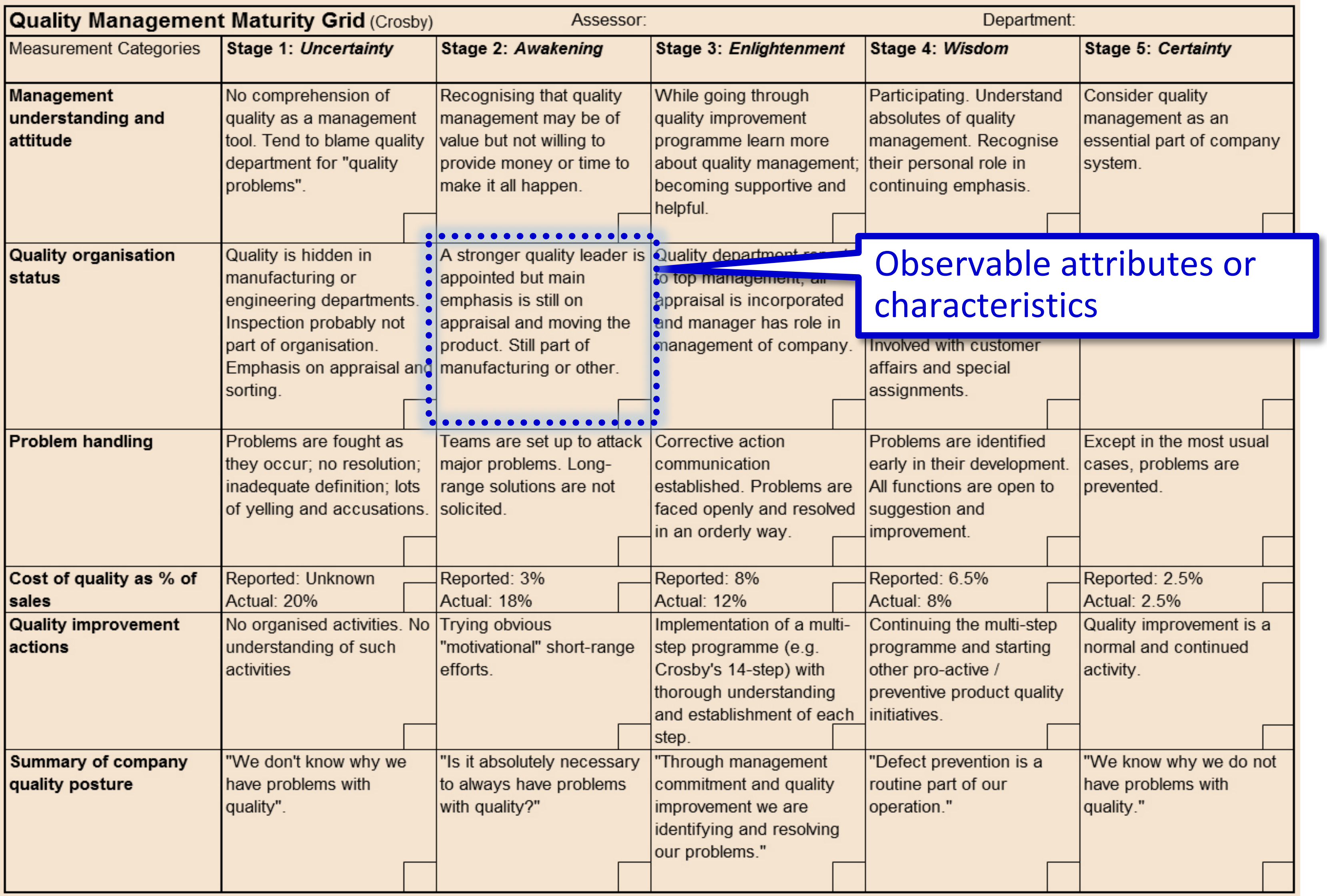
How to manage quality — so that it becomes a source of profit for your business

PHILIP B. CROSBY

author of:
"The Art of Getting Your Own Sweet Way"

- Viewed “quality” as a characteristic owned by everyone in the organization
- Created the Quality Management Maturity Grid to express organizational maturity across a range of quality attributes or categories
- Defined observable outcomes as benchmarks

The Quality Management Maturity Grid



Quality Management Maturity Grid (Crosby)		Assessor:		Department:	
Measurement Categories	**Stage 1: *Uncertainty***	**Stage 2: *Awakening***	**Stage 3: *Enlightenment***	**Stage 4: *Wisdom***	**Stage 5: *Certainty***
Management understanding and attitude	No comprehension of quality as a management tool. Tend to blame quality department for "quality problems".	Recognising that quality management may be of value but not willing to provide money or time to make it all happen.	While going through quality improvement programme learn more about quality management; becoming supportive and helpful.	Participating. Understand absolutes of quality management. Recognise their personal role in continuing emphasis.	Consider quality management as an essential part of company system.
Quality organisation status	Quality is hidden in manufacturing or engineering departments. Inspection probably not part of organisation. Emphasis on appraisal and sorting.	A stronger quality leader is appointed but main emphasis is still on appraisal and moving the product. Still part of manufacturing or other.	Quality department reports to top management, all appraisal is incorporated and manager has role in management of company.	[illegible] Involved with customer affairs and special assignments.	[illegible]
Problem handling	Problems are fought as they occur; no resolution; inadequate definition; lots of yelling and accusations.	Teams are set up to attack major problems. Long-range solutions are not solicited.	Corrective action communication established. Problems are faced openly and resolved in an orderly way.	Problems are identified early in their development. All functions are open to suggestion and improvement.	Except in the most usual cases, problems are prevented.
Cost of quality as % of sales	Reported: Unknown Actual: 20%	Reported: 3% Actual: 18%	Reported: 8% Actual: 12%	Reported: 6.5% Actual: 8%	Reported: 2.5% Actual: 2.5%
Quality improvement actions	No organised activities. No understanding of such activities	Trying obvious "motivational" short-range efforts.	Implementation of a multi-step programme (e.g. Crosby's 14-step) with thorough understanding and establishment of each step.	Continuing the multi-step programme and starting other pro-active / preventive product quality initiatives.	Quality improvement is a normal and continued activity.
Summary of company quality posture	"We don't know why we have problems with quality".	"Is it absolutely necessary to always have problems with quality?"	"Through management commitment and quality improvement we are identifying and resolving our problems."	"Defect prevention is a routine part of our operation."	"We know why we do not have problems with quality."

Observable attributes or characteristics

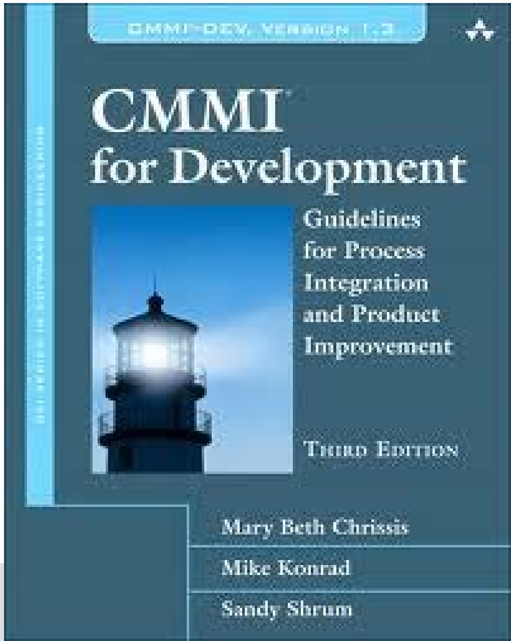
Evolution of the QMMG

1986 – Watts Humphrey formalizes the Process Maturity Framework into the Capability Maturity Model for Software (SW-CMM) at Carnegie Mellon’s Software Engineering Institute

Driven by USAF need to measure capabilities of software contractors

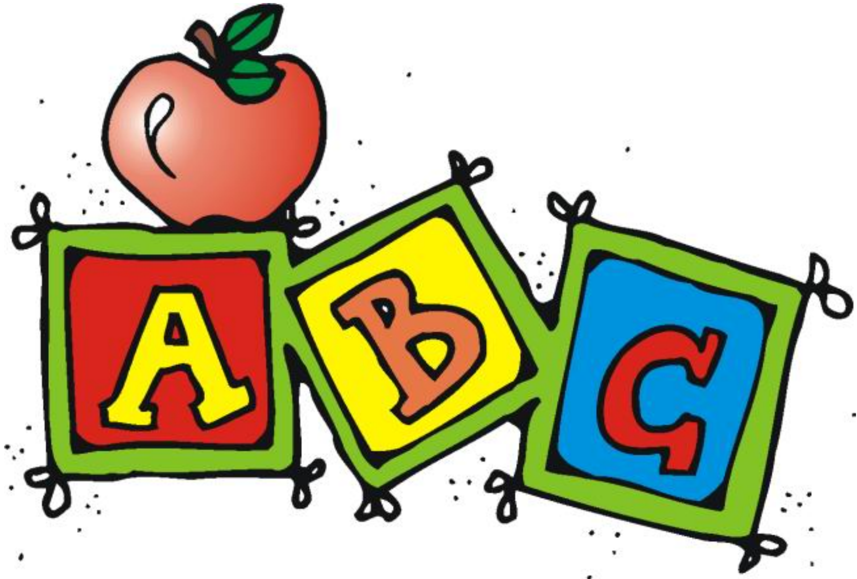
Architecturally based on the QMMG but reflective of observed best practices for software development

2000 - CMM Integration (CMMI) created to combine software, systems engineering and integrated product processes; now at v1.3



ABCs of Maturity Models

- What are maturity models?
- Types of maturity models
- Examples of maturity models

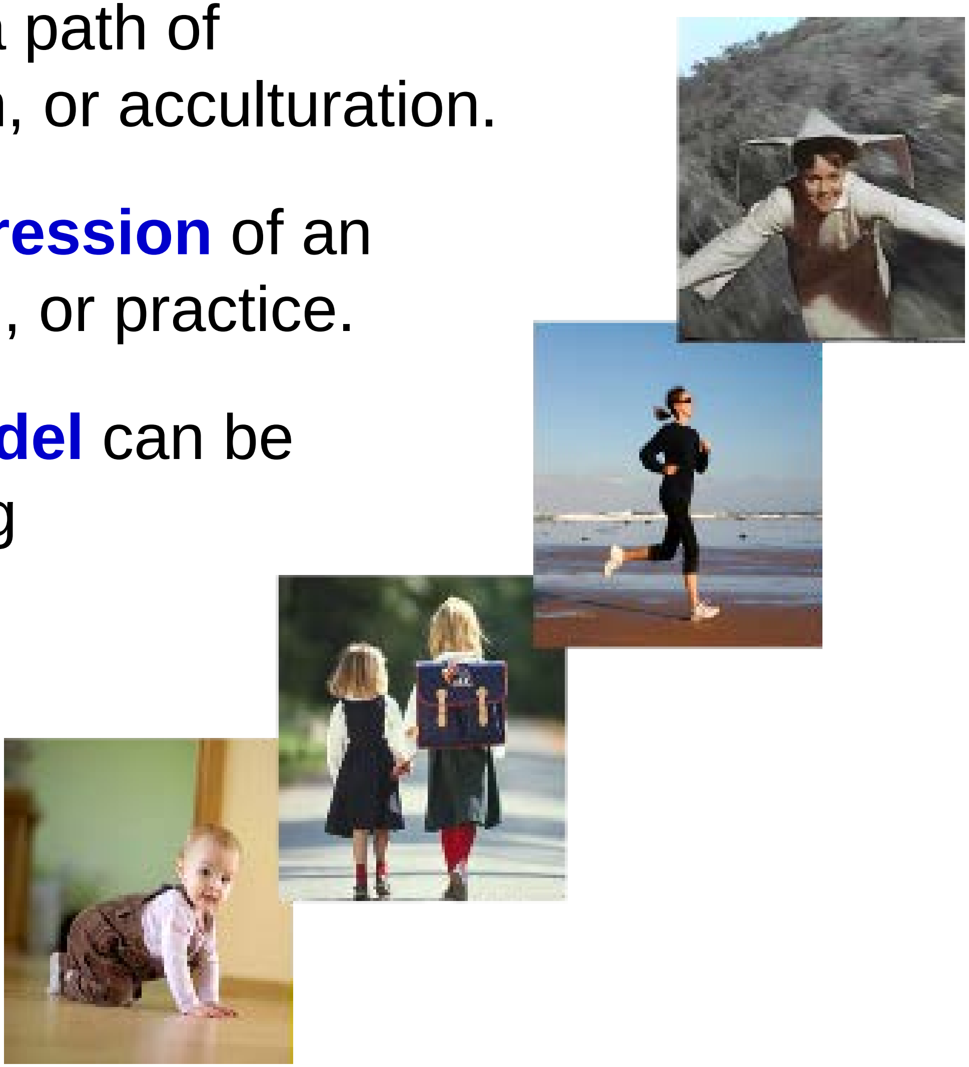


Maturity Model Defined

An **organized way** to convey a path of experience, wisdom, perfection, or acculturation.

Depicts an **evolutionary progression** of an attribute, characteristic, pattern, or practice.

The **subject of a maturity model** can be objects or things, ways of doing something, characteristics of something, practices, controls, or processes.



Maturity Models Provide…

Means for **assessing** and benchmarking performance

Ability to assess how a set of characteristics have **evolved**

Expression of a body of knowledge of **best practices**

Means to **identify gaps** and develop improvement plans

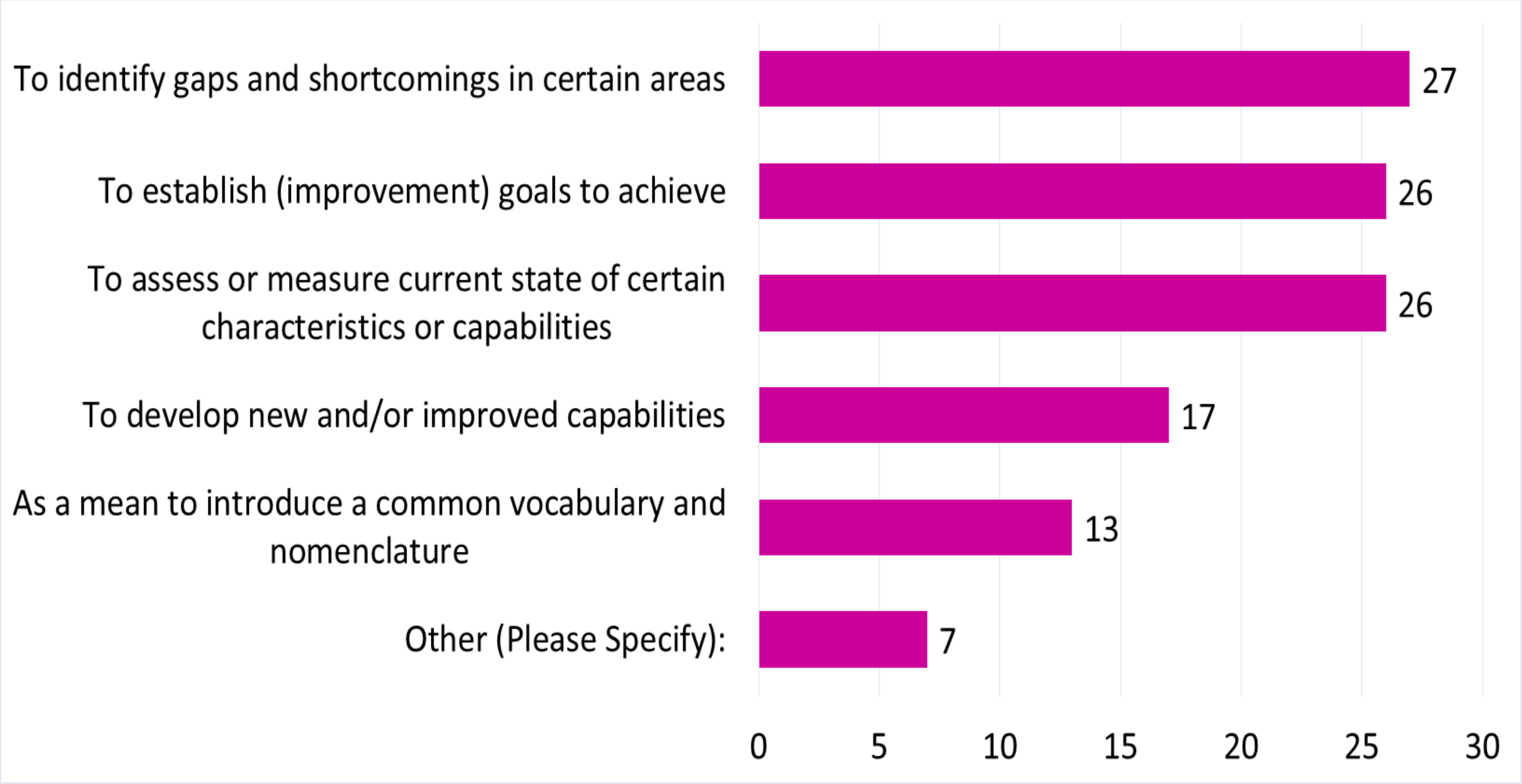
Roadmap for model-based **improvement**

Demonstrated **results** of improvement efforts

Common language or **taxonomy**

Maturity Models Member Query – Q3

For what purpose?



Maturity Models Member Query – Q3

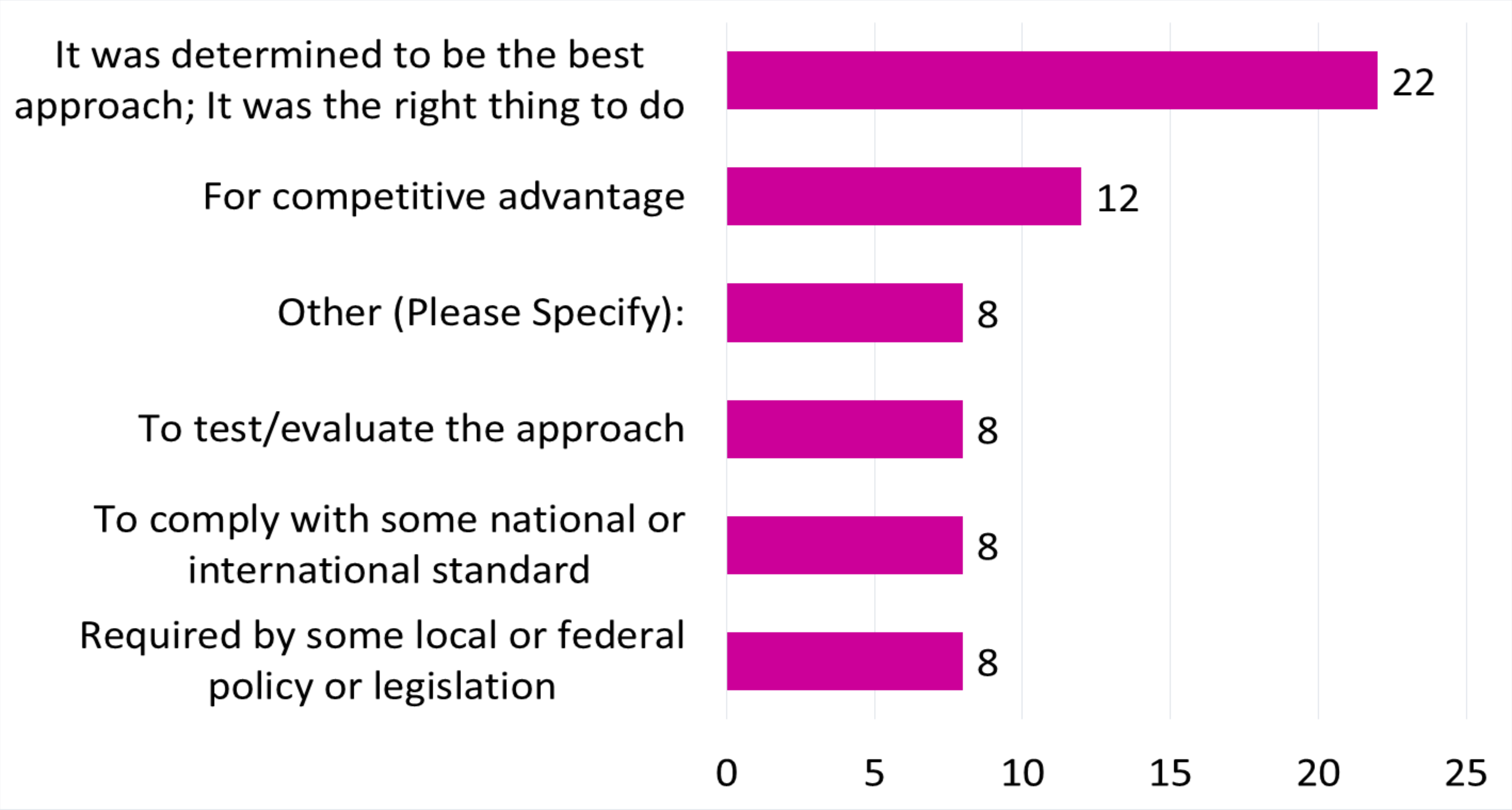
For what purpose?

OTHER:

- Governance
- To compare to other organizations
- Yes to all with emphasis on common vocabulary and driving to goals.
- Define strategic IA maturity objectives and develop an action plan for improvement
- Yes to all but the approaches vary considerably across the company

Maturity Models Member Query – Q4

For what reason?



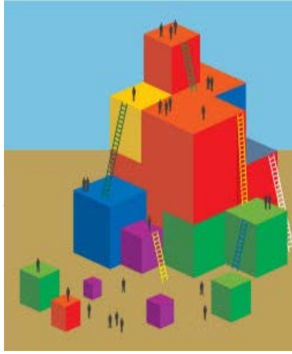
Maturity Models Member Query – Q4

For what reason?

OTHER:

- To help create strategy
- To develop capability
- To test and evaluate approach
- To communicate upwards
- To set expectations
- To communicate opportunity for improvement
- Mandated across UK Government Departments
- All; depending upon area of the company and various contract drivers.
- A combination of drivers towards pragmatic centralized management and scoring.
- Trying to establish a common method to develop roadmaps understandable by executive committee and board of directors

Key Components of a Maturity Model



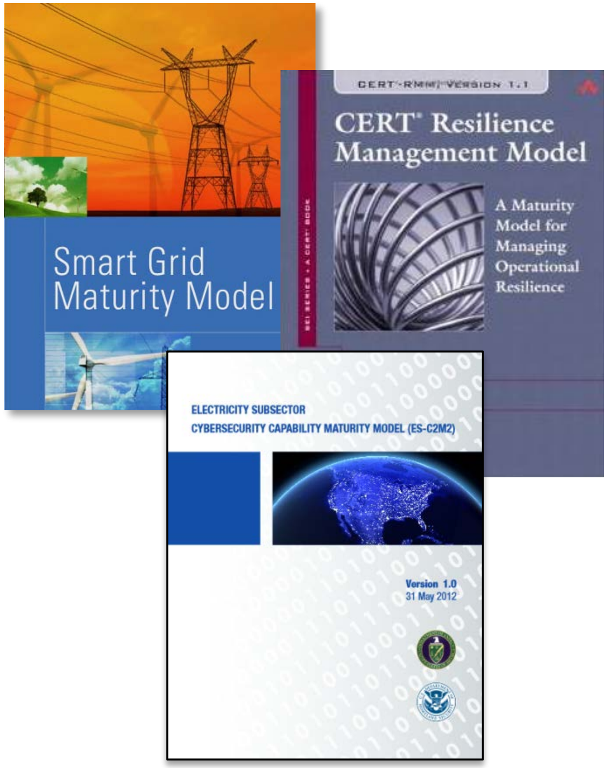
Levels	• The measurement scale • The transitional states
Domains	• Logical groupings of like attributes into areas of importance to the subject matter and intent of the model • Logical groupings of like practices, processes, or good things to do
Attributes	• Core content of the model arranged by domains and levels • Typically based on observed practices, standards, or expert knowledge
Diagnostic Methods	• For assessment, measurement, gap identification, benchmarking
Improvement Roadmaps	• To guide improvement efforts (Plan-Do-Check-Act; Observe-Orient-Decide-Act)

Types of Maturity Models

There are three types of maturity models

- Progression Maturity Models
- Capability Maturity Models (CMM)
- Hybrid Maturity Models

One or more may be appropriate for your particular needs


Smart Grid Maturity Model
CERT-RMM VERSION 1.1
CERT® Resilience Management Model
A Maturity Model for Managing Operational Resilience
SEI SERIES • A CERT® BOOK
ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)
Version 1.0
31 May 2012

⚠ **Not all maturity models are CMMs**

Progression Model Defined

Simple progression or scaling of an attribute, characteristic, pattern, or practice

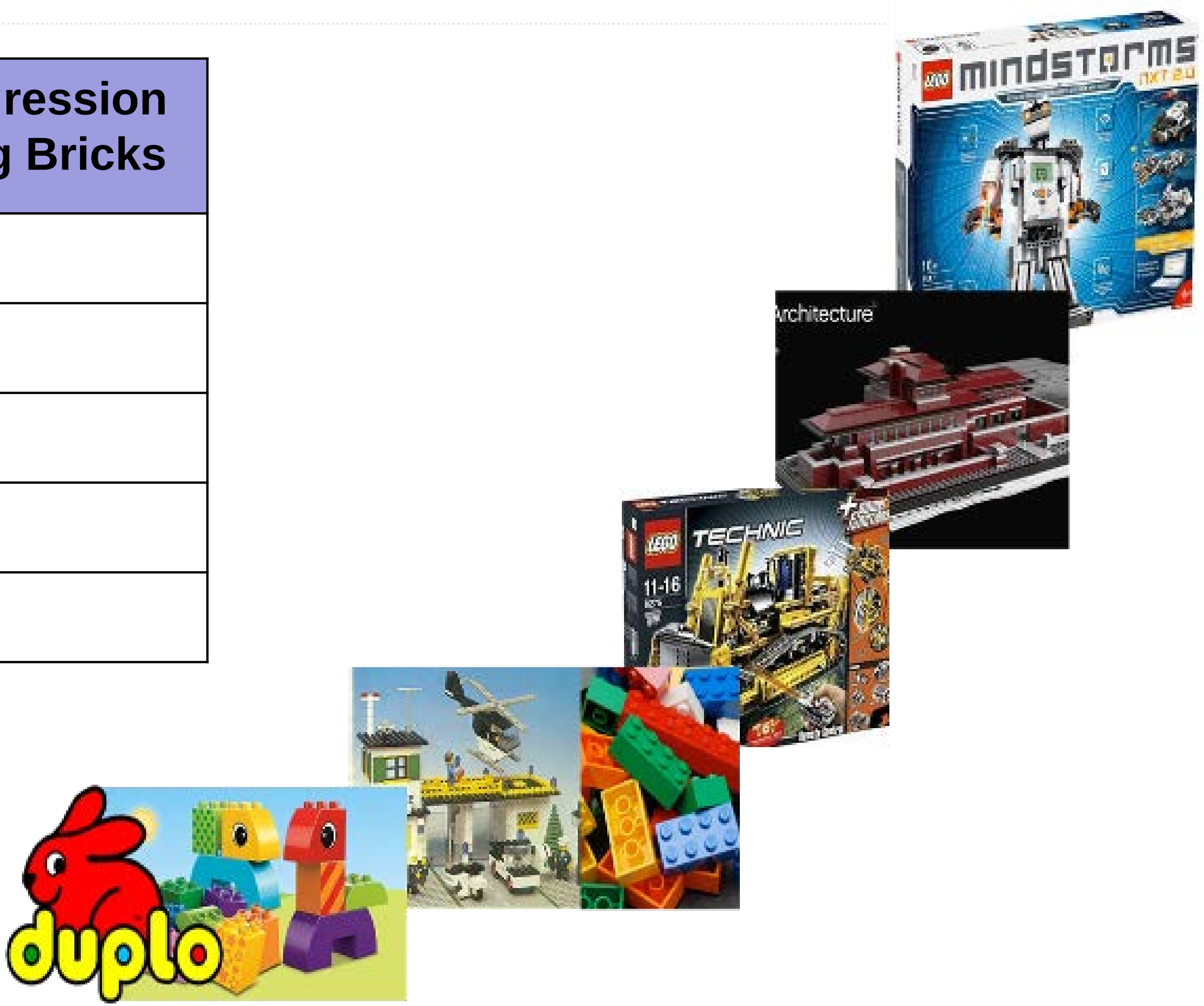
Levels describe higher states of achievement, advancement, completeness, or evolution

Levels can be agreed upon by users, industry, etc.

A Maturity Progression for Toy Building Bricks

Progression Model Example

A Maturity Progression for Toy Building Bricks
Lego Mindstorms
Lego Architecture
Lego Technic
Lego City
Lego Duplo



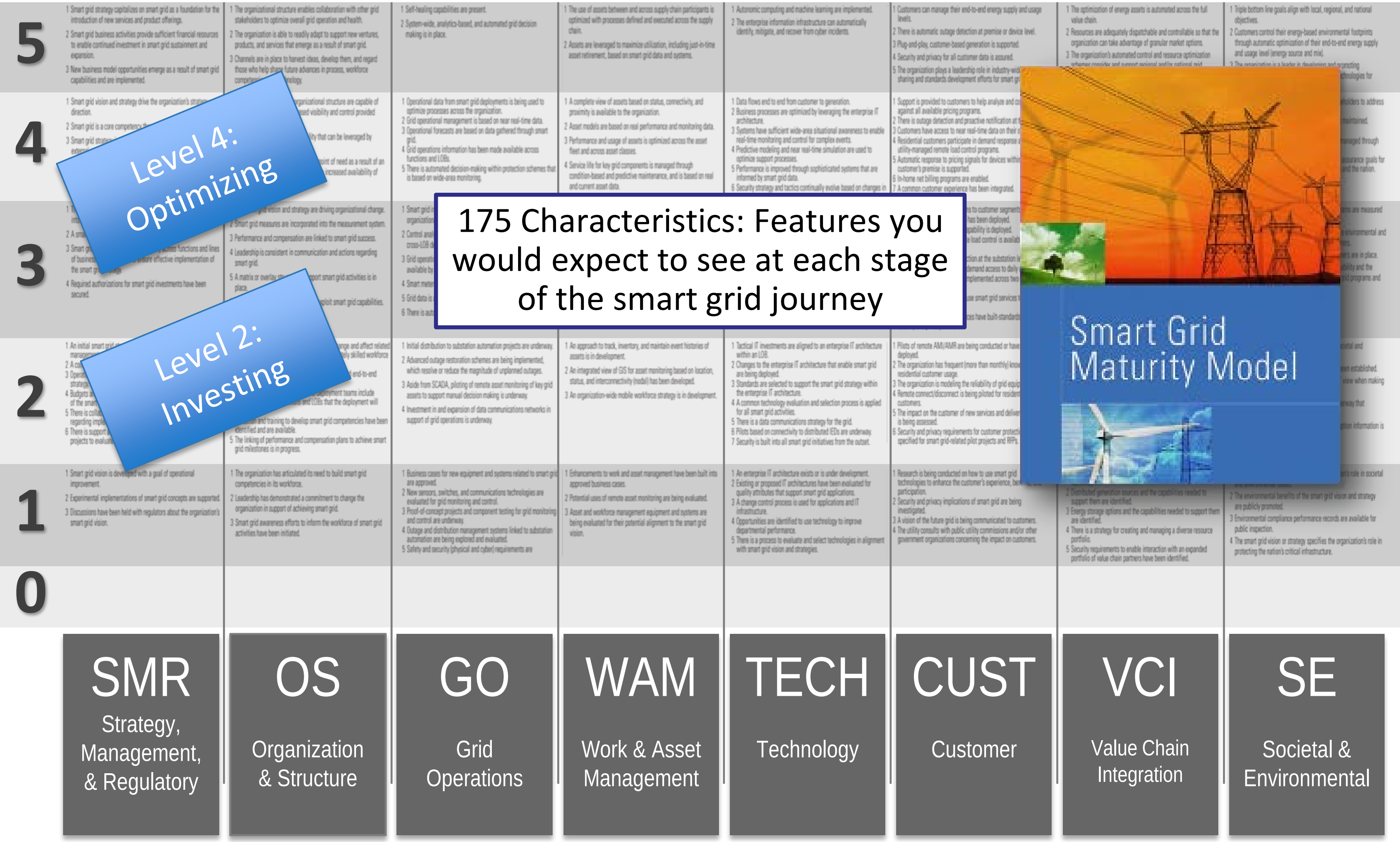
Progression Model Example *(cont.)*

A Maturity Progression for Counting
Computer
Calculator
Adding machine
Slide rule
Abacus
Pencil and paper
Sticks/Stones
Fingers

A Maturity Progression for Authentication
Three-factor authentication
Two-factor authentication
Addition of changing every 60 days
Use of strong passwords
Use of simple passwords

Progress does not necessarily equal process maturity

Progression Model Example: SGMM



5

4

3

2

1

0

Level 4: Optimizing

Level 2: Investing

175 Characteristics: Features you would expect to see at each stage of the smart grid journey

SMR	OS	GO	WAM	TECH	CUST	VCI	SE
Strategy, Management, & Regulatory	Organization & Structure	Grid Operations	Work & Asset Management	Technology	Customer	Value Chain Integration	Societal & Environmental

Benefits & Limitations of Progression Models

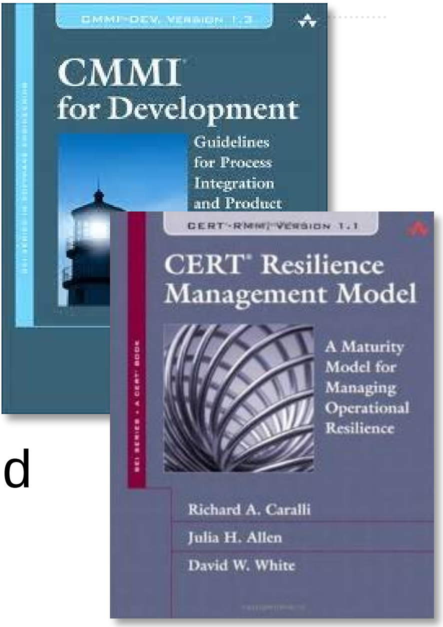
Benefits

- Provides a transformative roadmap
- Simple to understand and us
- Low adoption cost
- Easy to recalibrate as technologies and practices advance

Limitations

- Levels could be arbitrarily defined
  - Okay, as long as applied consistently.
- Achieving higher levels of "practice maturity" does not necessarily translate into "process maturity"
- Often confused with CMMs - thus users inaccurately project traits of CMMs on progression models

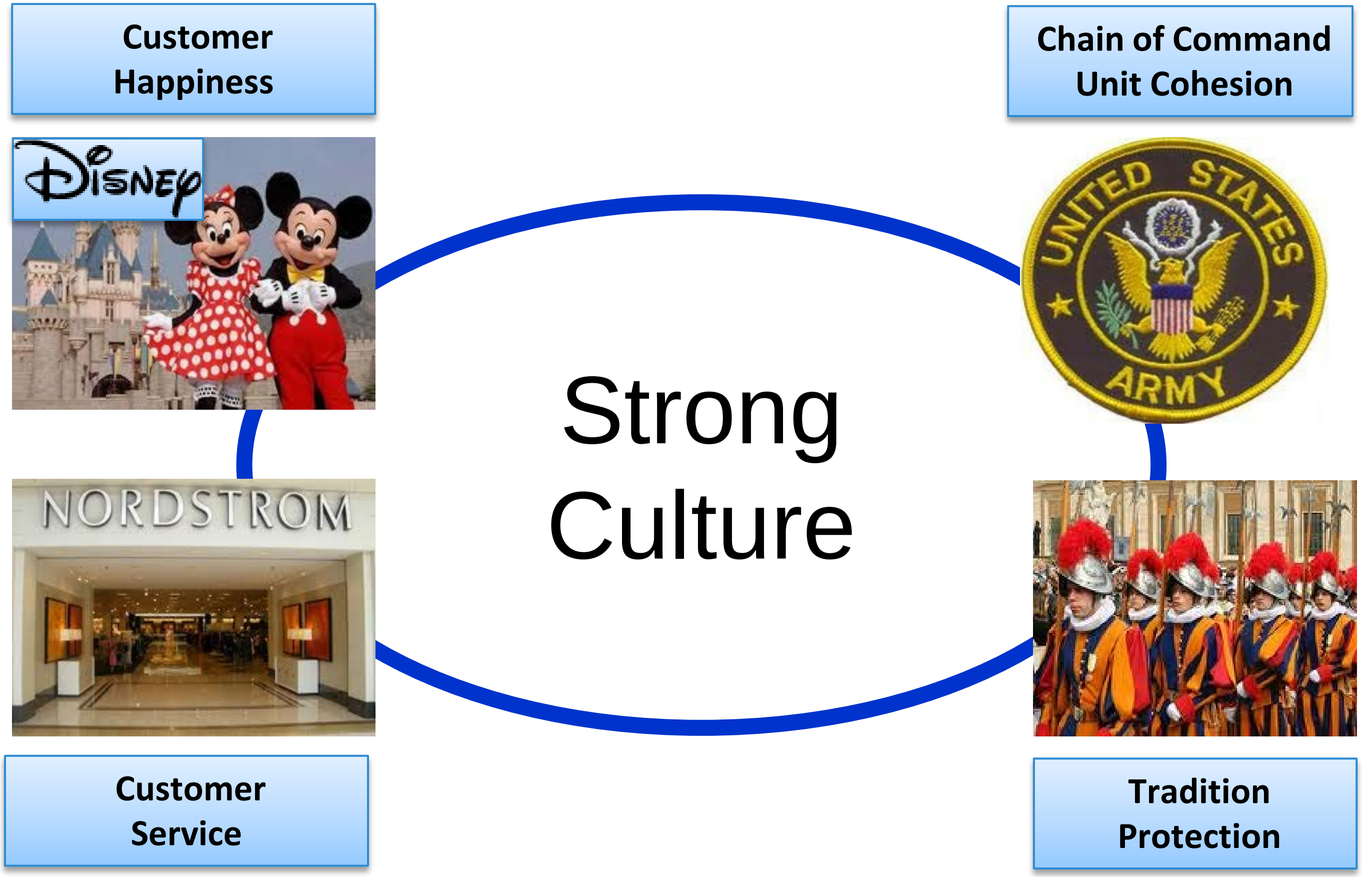
Capability Maturity Models (CMM)


CMMI-DEV, VERSION 1.3
CMMI for Development
Guidelines for Process Integration and Product
CERT-RMM, VERSION 1.1
CERT Resilience Management Model
A Maturity Model for Managing Operational Resilience
Richard A. Caralli
Julia H. Allen
David W. White

- A more complex instrument
- Characterizes
  - the maturity of processes
  - the maturity of the culture of the organization
  - the degree to which processes are institutionalized
  - the extent to which the organization demonstrates process maturity
- Levels reflect the extent to which a particular set of practices have been institutionalized
  - Institutionalized processes are more likely to be retained during times of stress.

Progression of Process Institutionalization

What Do These Organizations Have in Common?



Customer Happiness

Chain of Command
Unit Cohesion

Strong Culture

Customer Service

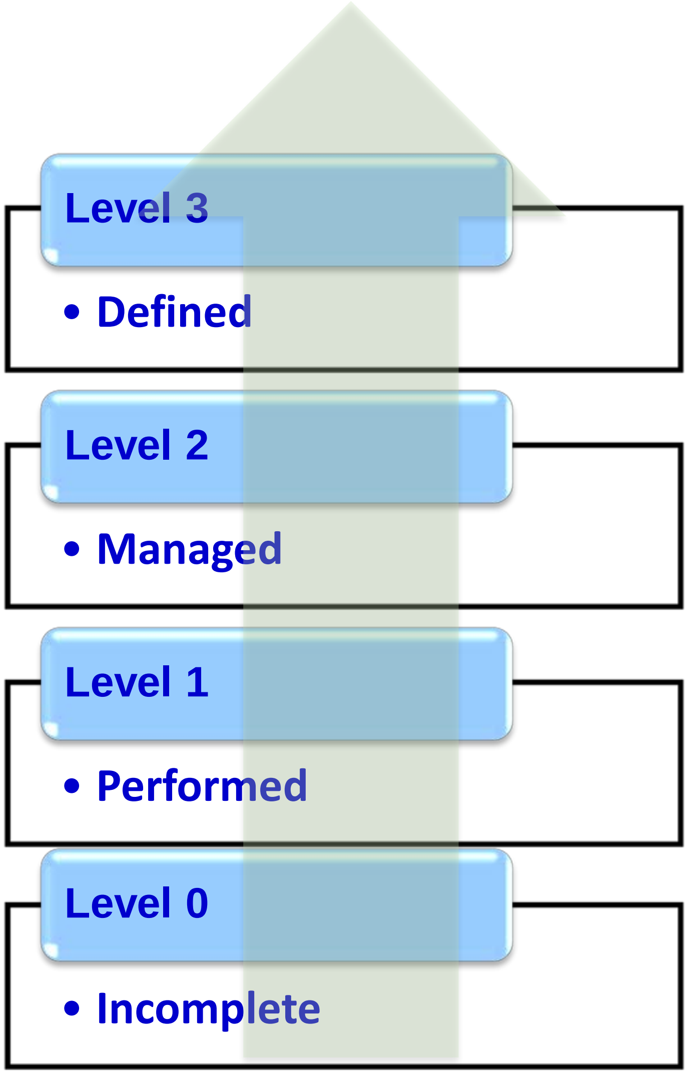
Tradition
Protection

Capability Maturity Model Levels

Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete



Level 3

- Defined

Level 2

- Managed

Level 1

- Performed

Level 0

- Incomplete

Higher degrees of institutionalization translate to more stable processes that

- *are repeatable*
- *produce consistent results over time*
- *are retained during times of stress*

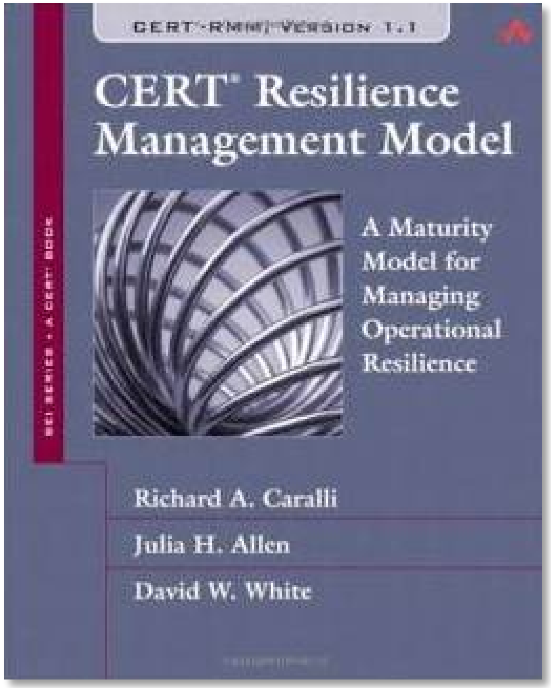
Examples of CMM Levels

Example 1
Optimized
Quantitatively Managed
Defined
Managed
Ad hoc

Example 2
Externally integrated
Internally integrated
Managed
Performed
Initiated

Example 3
Shared
Defined
Measured
Managed
Planned
Performed but ad hoc
Incomplete

Capability Maturity Model Example: CERT-RMM *(1 of 6)*



CERT-RMM VERSION 1.1

CERT® Resilience Management Model

A Maturity Model for Managing Operational Resilience

Richard A. Caralli

Julia H. Allen

David W. White

Framework for managing and improving operational resilience

http://www.cert.org/resilience/

"…an extensive super-set of the things an organization could do to be more resilient."

- CERT-RMM adopter

CERT-RMM *(2 of 6)*

Operational Resilience Perspective

- The **emergent** property of an entity that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

Disruptions come from realized risk

- Natural or manmade
- Accidental or intentional
- Small or large
- Information technology or not
- Cyber or kinetic

CERT-RMM *(3 of 6)*

- Cybersecurity, business continuity, IT disaster recovery are risk management processes
- For operational risk management to be effective, these activities must work toward the same goals
- Operational resilience emerges from effective operational risk management

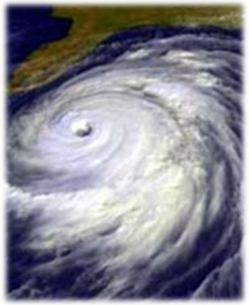
Actions of people

```
A fatal exception
000059F8. The curr

* Press any key to
* Press CTRL+ALT+D
  lose any unsaved
```

Systems and technology failures

Failed internal processes



External events

CERT-RMM *(4 of 6)*

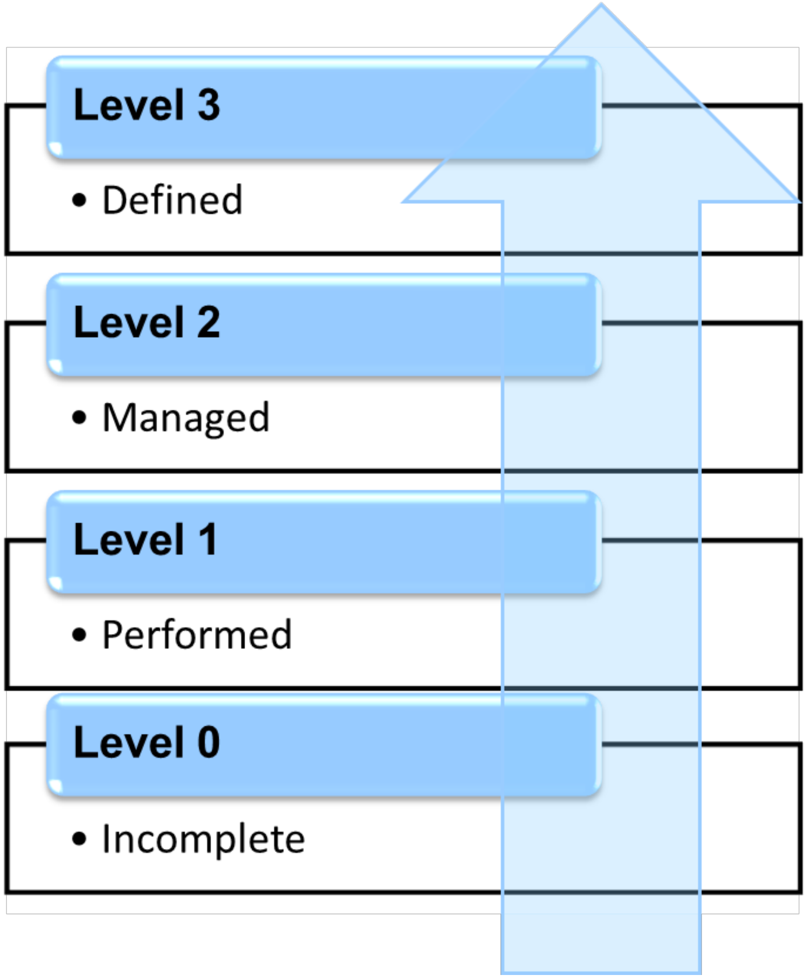
- Most comprehensive framework for managing and improving operational resilience
- Guides implementation and management of operational resilience activities
- Enables and promotes the **convergence** of
  - COOP, IT Disaster Recovery, Business Continuity
  - Information Security, Cybersecurity
  - IT Operations

CERT-RMM Process Areas (Domains) *(5 of 6)*

- Access Management
- Asset Definition and Management
- Communications
- Compliance
- Controls Management
- Enterprise Focus
- Environmental Control
- External Dependencies Management
- Financial Resource Management
- Human Resource Management
- Identity Management
- Incident Management & Control
- Knowledge & Information Management

- Measurement and Analysis
- Monitoring
- Organizational Process Definition
- Organizational Process Focus
- Organizational Training & Awareness
- People Management
- Resilience Requirements Development
- Resilience Requirements Management
- Resilient Technical Solution Engineering
- Risk Management
- Service Continuity
- Technology Management
- Vulnerability Analysis & Resolution

CERT-RMM Capability Levels *(6 of 6)*



Level 3

- Defined

Level 2

- Managed

Level 1

- Performed

Level 0

- Incomplete

Processes are acculturated, defined, measured, and governed

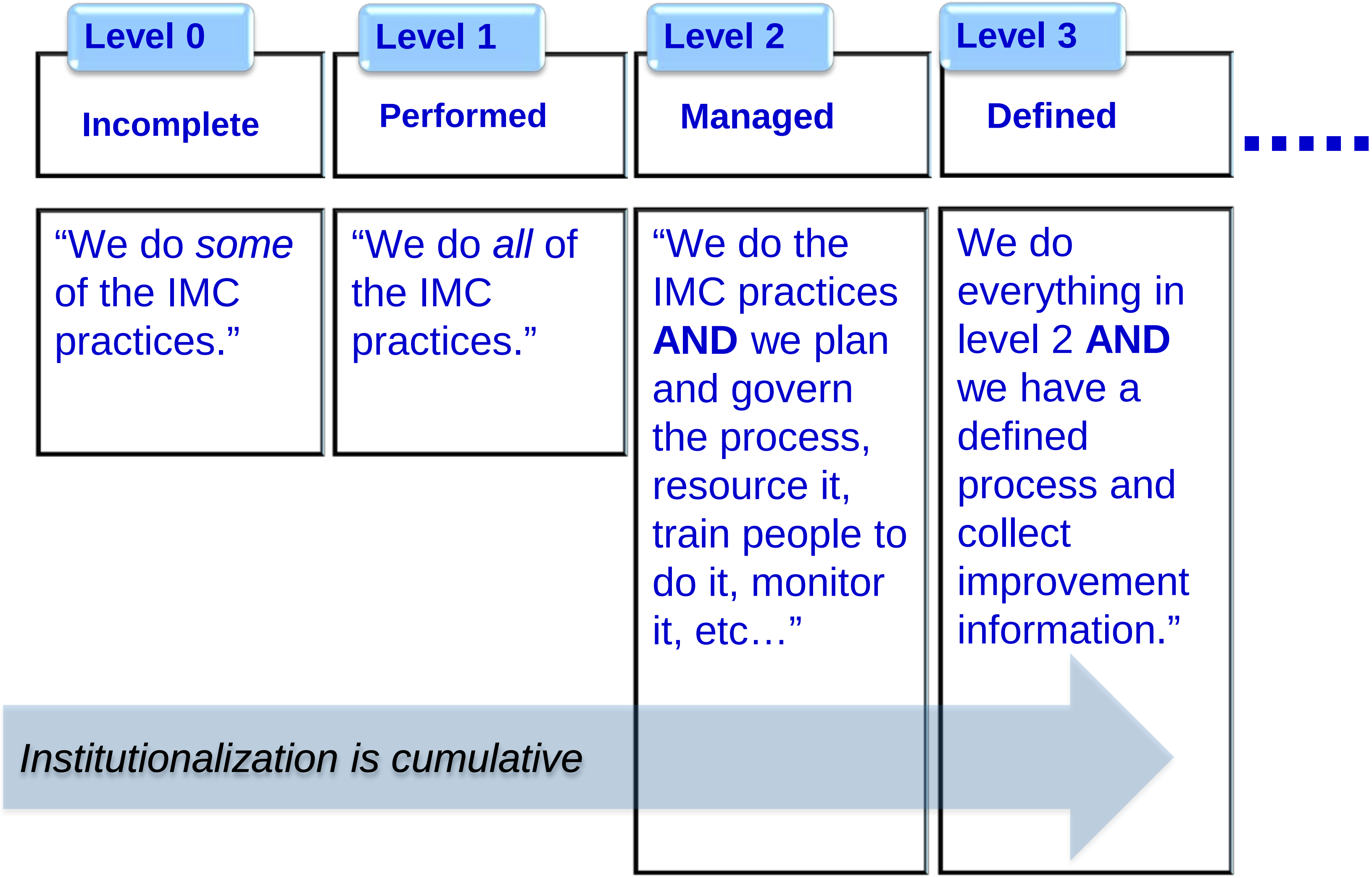
Practices are performed

Incident Management & Control: An Example

Consider the **Incident Management and Control (IMC)** domain from CERT-RMM:

- Goal 1: Establish the IMC process
- Goal 2: Detect events
- Goal 3: Declare incidents
- Goal 4: Respond to and recover from incidents
- Goal 5: Establish incident learning

Incident Management by the CMM Levels



Level 0

Incomplete

“We do *some* of the IMC practices.”

Level 1

Performed

“We do *all* of the IMC practices.”

Level 2

Managed

“We do the IMC practices **AND** we plan and govern the process, resource it, train people to do it, monitor it, etc…”

Level 3

Defined

We do everything in level 2 **AND** we have a defined process and collect improvement information.”

Institutionalization is cumulative

Benefits and Limitations of CMMs

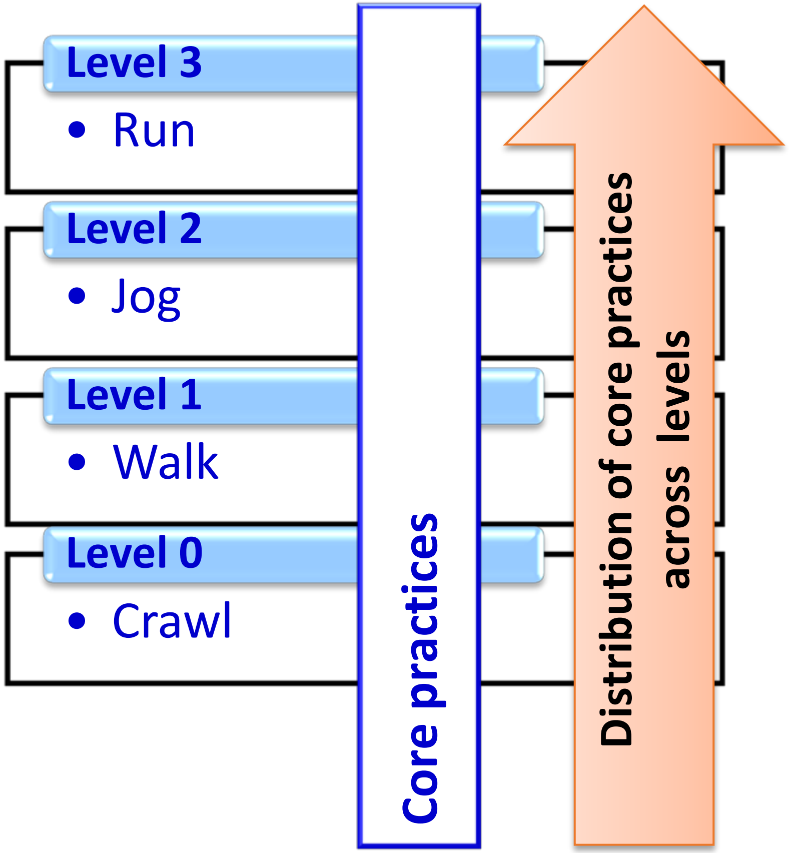
Benefits

- Provides for measurement of core competencies
- Provides for rigorous measurement of capability—the ability to retain core competencies under times of stress
- Can provide a path to quantitative measurement

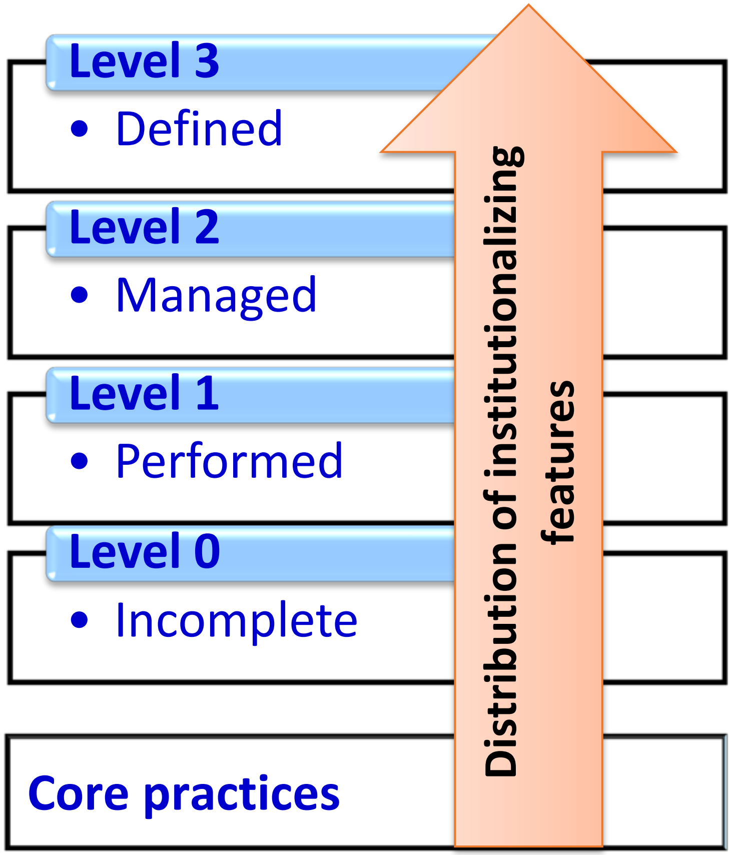
Limitations

- Sometimes difficult to understand and apply; high adoption cost
- “Maturity” may not translate into actual results
- Potential false sense of achievement: achieving high maturity in security practices may not mean the organization is “secure” enough
- You can achieve high maturity ratings in a capability model by institutionalizing ineffective, poorly-designed, or inefficient processes.

Compare: Progression vs CMM



Progression Model



Capability Model

Hybrid Models

Combine best features of progression and capability maturity models

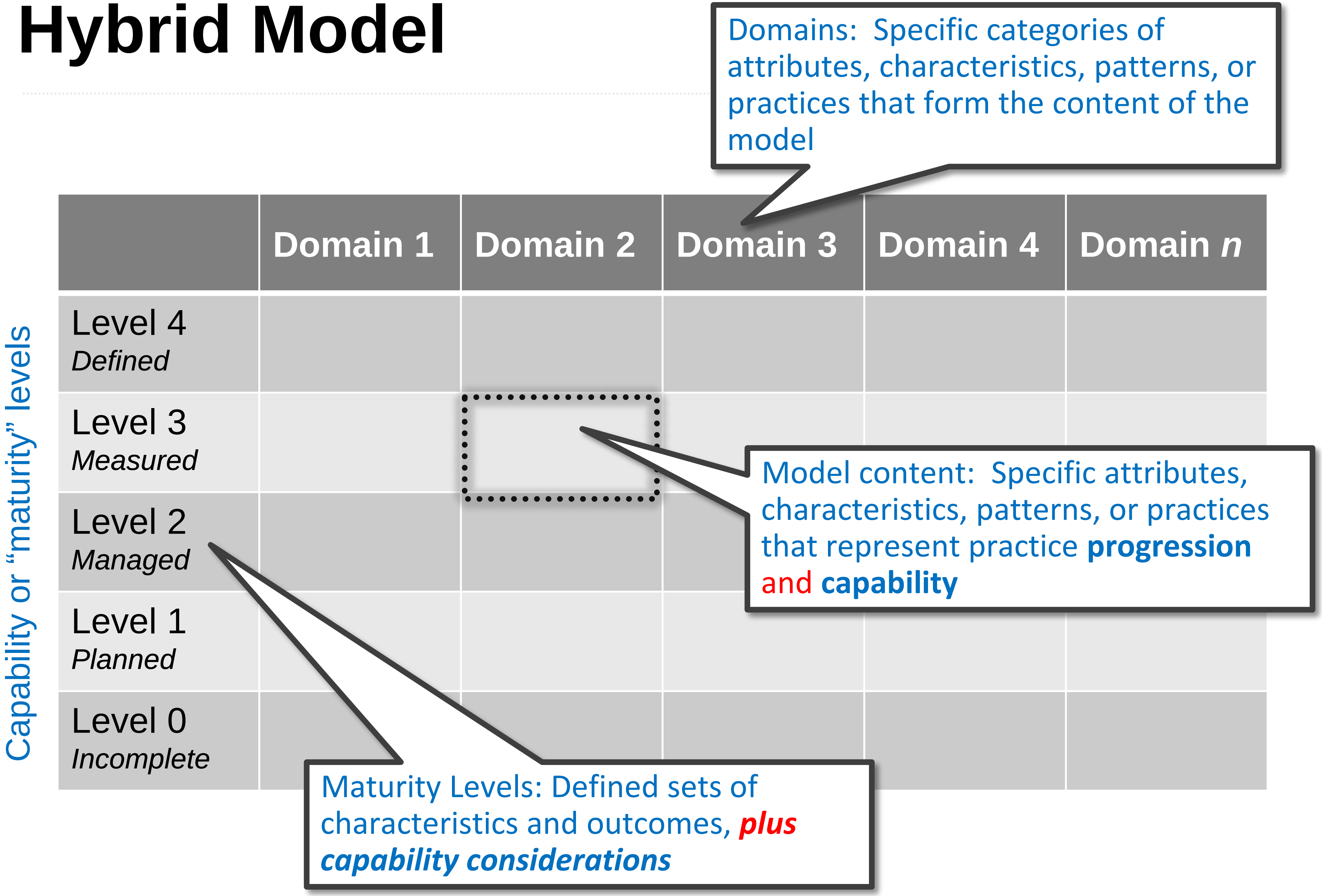
- Allow for measurement of evolution or achievement as in progression models
- Add the ability to measure capability or institutionalization with the rigor of a CMM

Levels reflect both achievement and capability

Transitions between levels:

- Similar to a capability model (i.e., describe capability maturity)
- Architecturally use the characteristics, indicators, attributes, or patterns of a progression model

Hybrid Model



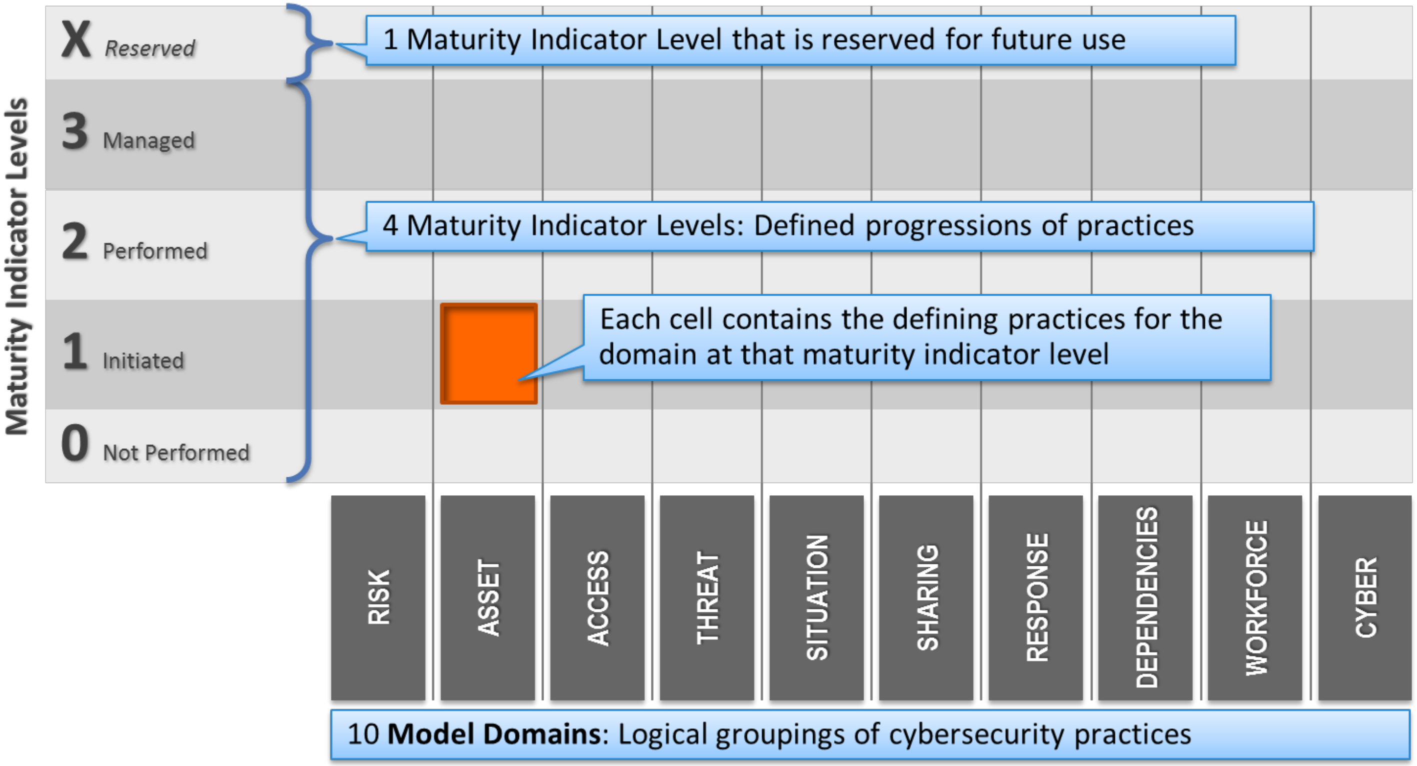
Domains: Specific categories of attributes, characteristics, patterns, or practices that form the content of the model

	Domain 1	Domain 2	Domain 3	Domain 4	Domain *n*
Level 4 *Defined*					
Level 3 *Measured*					
Level 2 *Managed*					
Level 1 *Planned*					
Level 0 *Incomplete*					

Model content: Specific attributes, characteristics, patterns, or practices that represent practice **progression** and **capability**

Maturity Levels: Defined sets of characteristics and outcomes, ***plus capability considerations***

Hybrid Model Example: ES-C2M2 *(1 of 3)*



Maturity Indicator Levels

X *Reserved*

3 Managed

2 Performed

1 Initiated

0 Not Performed

1 Maturity Indicator Level that is reserved for future use

4 Maturity Indicator Levels: Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level

RISK

ASSET

ACCESS

THREAT

SITUATION

SHARING

RESPONSE

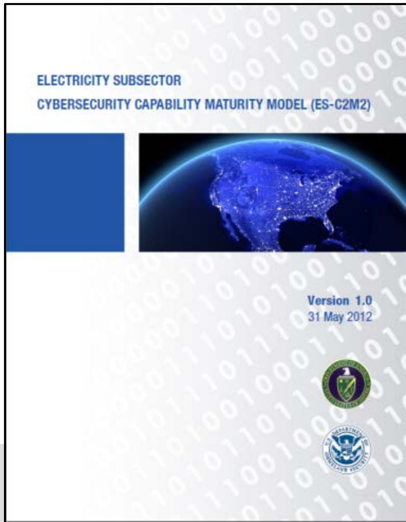
DEPENDENCIES

WORKFORCE

CYBER

10 **Model Domains**: Logical groupings of cybersecurity practices

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



ELECTRICITY SUBSECTOR

CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

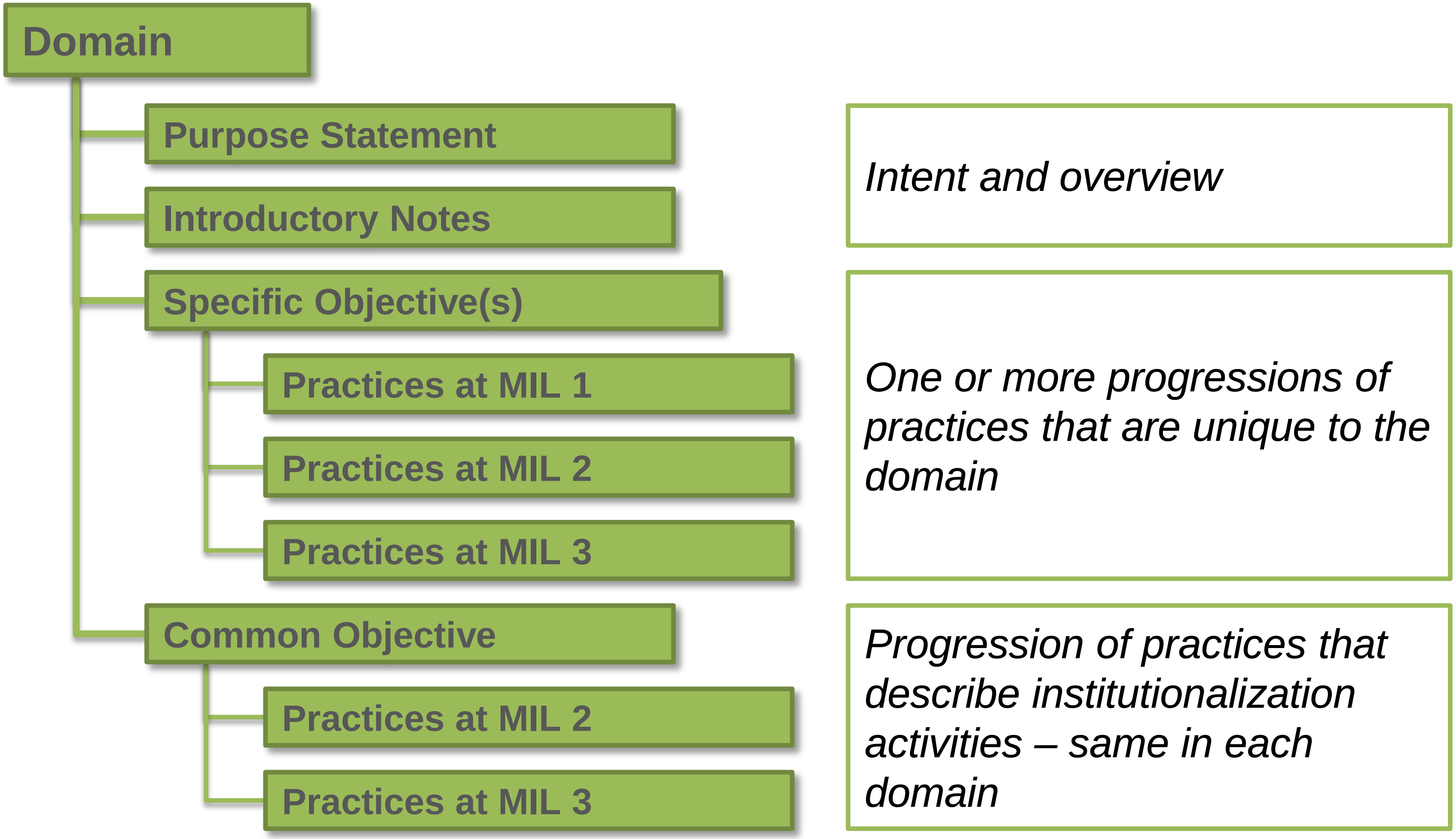
Version 1.0

31 May 2012

Hybrid Model Example: ES-C2M2 *(2 of 3)*

Level	Name	Characteristics
MIL0	Not Performed	- Practices are not performed
MIL1	Initiated	- Initial practices are performed but may be ad hoc
MIL2	Performed	**Approach characteristic:** - Practices are more complete or advanced than at MIL1 **Institutionalization characteristics:** - Practices are documented - Stakeholders are identified and involved - Adequate resources are provided to support the process - Standards or guidelines are used to guide practice implementation
MIL3	Managed	**Approach characteristic:** - Practices are more complete or advanced than at MIL2 **Institutionalization characteristics:** - Activities are guided by policy (or other directives) and governance - Policies include compliance requirements for specified standards or guidelines - Activities are periodically reviewed for conformance to policy - Responsibility and authority for practices are assigned to personnel - Personnel performing the practice have adequate skills and knowledge

Hybrid Model Example: ES-C2M2 *(3 of 3)*



Domain

- Purpose Statement
- Introductory Notes
- Specific Objective(s)
  - Practices at MIL 1
  - Practices at MIL 2
  - Practices at MIL 3
- Common Objective
  - Practices at MIL 2
  - Practices at MIL 3

Intent and overview

One or more progressions of practices that are unique to the domain

Progression of practices that describe institutionalization activities – same in each domain

Benefits and Limitations of Hybrid Models

Benefits

- Provides for easy measurement of core competencies as well as approximation of capability
- Can adapt easily to evolution of technologies and practices without sacrificing capability measurement
- Low adoption cost

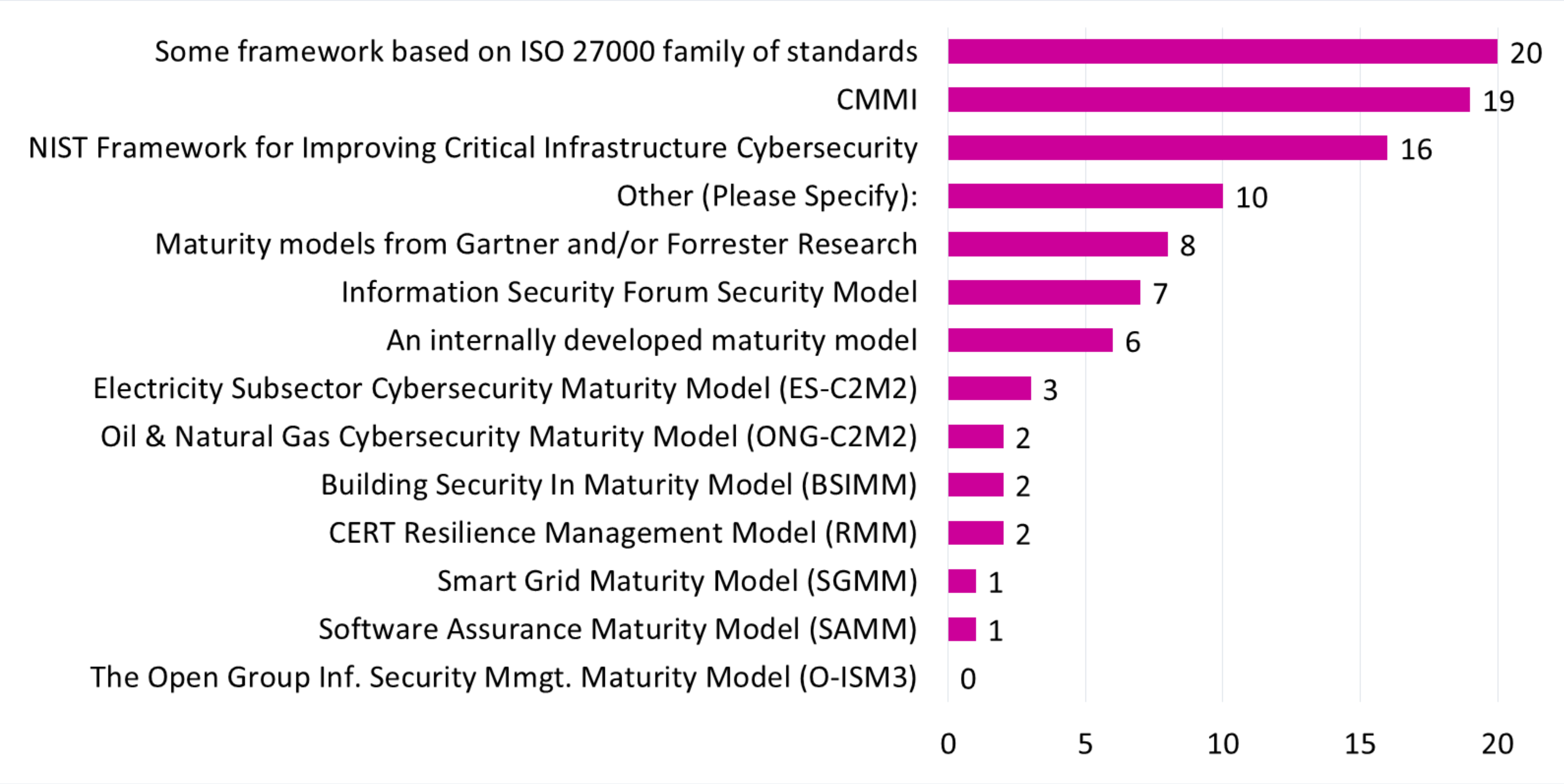
Limitations

- "Maturity" concept is approximated; not as rigorous as CMM
- Combination of attributes with institutionalizing features at each level can be arbitrary
  - Okay, as long as applied consistently.

Comparison of Frameworks	Progression MM	Capability MM	Hybrid MM	Code of Practice	Other
Smart Grid Maturity Model (SGMM)	x				
Versions of COBIT Prior to Version 5	x				
Building Security In Maturity Model (BSIMM)	x				
Gartner ITScore for Infrastructure and Operations	x				
Forrester Information Security Maturity Model	x				
CMMI Resilience		x			
CERT® Resilience Management Model (CERT-RMM)		x			
COBIT Version 5		x			
Software Assurance Maturity Model (SAMM)		x			
The Open Group Info. Security Management Maturity Model (O-ISM3)		x			
Electricity Subsector Cybersecurity Maturity Model (ES-C2M2)			x		
Oil & Natural Gas Cybersecurity Maturity Model (ONG-C2M2)			x		
Some framework based on ISO 27000 family of standards				x	
Information Security Forum Standard of Good Practice for Info. Security				x	
NIST Framework for Improving Critical Infrastructure Cybersecurity					x

Maturity Models Member Query – Q5

Which maturity models?



Maturity Models Member Query – Q5

Which maturity models?

OTHER:

- WEF
- COBIT
- COBIT
- COBIT
- Proprietary
- A blend of several
- SANS top 20 critical controls
- HMG Information Assurance Maturity Model
- Internally developed model based on COBIT

Maturity Models Member Query – Q6

If no, how do you assess the maturity of your cybersecurity program?

- In an ad hoc manner
- Best of breed analytics
- We are intending to use an external consultancy that benchmarks to the NIST Cybersecurity framework.

Panel Discussion

- Real-life Examples
- Success Stories
- Lessons Learned
- Recommendations

Planned Members' Opening Remarks

Ben Krutzen

Shell

Jason Christopher

U.S. Department of Energy

David White

Axio Global

Question/Answer Session with the Panel

Ben Krutzen

Shell

Jason Christopher

U.S. Department of Energy

David White

Axio Global

Closing Thoughts

- Summary
- A few cautions
- Determining when and which type to use

First and Foremost

- Have a clear understanding of your business objectives for using any type of improvement model
  - — How the model will meet these objectives
- Understand how this initiative fits with others that are mainstream for the organization (not a new add-on)
- Have visible sponsorship of executives and senior leaders who are essential for success
- Have well-defined outcome measures that are regularly reported and reviewed
- Have a plan and committed resources

A Few Cautions

Progression models may be easier to adopt but may not be sustainable (aka sticky)

Definitions of levels can be arbitrary

- and, therefore, important to ensure consistency over time and/or over instances of being applied

Measuring process performance and maturity is useful but may not be sufficient

Exercise care when using maturity models for specific purposes

Progression Models May Not Be Sustainable

A progression model provides a roadmap or scale of a particular characteristic, indicator, attribute, pattern, or practice

- Focuses on practices or controls and their progression from least mature to most mature
- Cannot be used to measure the extent to which an organization is capable of sustaining the practice in times of disruption and stress (the practice has not become part of the DNA)

A hybrid or capability maturity model adds the dimension of organizational capability to practice progression

- Thus able to measure an organization's "resilience" in the presence of disruption and stress

Definitions of Levels and the Scale

Often defined by consensus of subject matter experts

Can simply reflect a plateau or a place in a progression or scale

Often have not been validated or are difficult to validate based on experience and measurement

May neglect to represent the capability and capacity of an organization to sustain operations in the presence of disruption and stress

Arbitrarily defined levels are fine so long as the scale is applied consistently:

- over time (e.g., to measure improvement)
- over instances (e.g., for benchmarking)

Measuring Process Performance May Not Be Sufficient

Experience demonstrates that the quality of the process directly affects the quality of the product

- However, process performance and maturity are only one aspect

Also need to consider the performance and maturity of

- The product and its outcomes
- The supporting technologies
- The environment within which the product operates
- Knowledge, skills, and abilities of people with respect to all of these
- Which of these dimensions to emphasize given product objectives

You can achieve high maturity ratings in a capability model by institutionalizing ineffective, poorly-designed, or inefficient processes.

When Does It Make Sense to Use Maturity Models?

Requirement for a structured approach

Demonstrated, measurable results based on an established body of knowledge

A defined roadmap from a current state to a desired state

An ability to monitor and measure progress, particularly in the presence of change

- Response to a strategic improvement or new product/new market objective

When Does It Make Sense to Use Maturity Models? *(cont.)*

Desire to answer these questions in a repeatable, predictable manner:

- How do I compare with my peers? (ability to benchmark)
- How can I determine how secure I am and if I am secure enough?
- How do I measure my current state? Characterize my desired state?
- What concrete actions do I need to take to improve? And in what order?
- How do I measure progress toward my desired state?
- How do I adapt to change?

Exercise Care When Using Maturity Models

If the immediate need is to respond to an in-progress disruptive event

- Robust processes are not yet in place
- Current protection and defensive mechanisms are failing
- Need to stop the bleeding, stabilize operations, rely on experts

In response to current and new compliance requirements

- In a highly regulated industry
- Must demonstrate compliance with specific laws, regulations and standard(s)
- Standard, defined processes and mapping new compliance requirements to these can be quite effective

Thank you for your attention…

References

- Caralli, R. A.; Allen, J. H.; & White, D. W. *The CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.
- CERT-RMM web site: http://www.cert.org/resilience/products-services/cert-rmm/index.cfm
- ES-C2M2 web site: http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity
- SGMM web site: http://www.sei.cmu.edu/smartgrid/